ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

Технологія управління привілейованим доступом користувачів інформаційної системи організації на базі Privilege Manager рішення Delinea

Виконав студент 6 курсу, групи БСЗМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Прус Кирило Володимирович
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NIST - Національний інститут стандартів і технологій США

COBIT - Control Objectives for Information and Related Technology

PAM - Privileged Account Management

SRM- security and risk management

PASM - Privileged account and session managemen

PSM - Privileged session management

PEDM - Privilege elevation and delegation management

SM - Secrets management

SoD - Separation of Duties

СКПП – система контролю привілейованих користувачів

SSC – хмарна архітектура Secret Server

ВСТУП

Актуальність дослідження. Керування привілейованими обліковими даними (PAM) — це домен у межах управління ідентифікацією та доступом (IdAM), який зосереджується на моніторингу та контролі використання привілейованих облікових даних. До привілейованих облікових даних належать локальні та доменні адміністративні облікові записи, екстрені облікові записи, облікові записи керування програмами та облікові записи служби. Ці облікові записи забезпечують розширений, часто необмежений, доступ до основних IT-ресурсів і технологій, тому зовнішні та внутрішні зловмисники прагнуть отримати до них доступ. Дуже важливо відстежувати, перевіряти, контролювати та управляти використанням привілейованими обліковими даними.

Організації можуть додати рівень безпеки між користувачами та привілейованими обліковими записами, до яких вони мають доступ, і включає типові сценарії використання для вирішення конкретних проблем, з якими стикається організація. Архітектура PAM показує, як моніторинг, аудит і елементи управління автентифікацією можуть поєднуватися, щоб запобігти несанкціонованому доступу та дозволити швидке виявлення несанкціонованого використання привілейованих облікових даних. Таким чино необхідно визначити методи та засоби управління привілейованими даними інформаційної системи організації. Це дозволить запобігти несанкціонованому доступу до інформаційної системи організації. Вищенаведені аргументи актуалізують дослідження щодо управління привілейованими даними інформаційної системи організації.

Об’єкт дослідження – процес управління привілейованим доступом інформаційної системи організації.

Предмет дослідження – технологія управління привілейованим доступом інформаційної системи організації.

Мета роботи – розробити варіанти технології управління привілейованим

доступом інформаційної системи організації та рекомендації щодо застосування технології в організації.

Наукові завдання:

- провести аналіз необхідності захисту привілейованих даних користувачів інформаційної системи організації;
- визначити основні проблеми привілейованого доступу користувачів інформаційної системи організації;
- проаналізувати методи та засоби управління привілейованим доступом користувачам інформаційної системи організації;
- розробити варіант технології управління привілейованим доступом користувачами інформаційної системи організації та розробити рекомендації фахівцям з кібербезпеки щодо застосування обраної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту привілейованих даних користувачів інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці варіанту основних компонентів технології Privilege Manager Delinea щодо управління доступом привілейованих користувачів інформаційної системи організації та розробці рекомендацій щодо використання даної технології в метою виявлення порушень з боку привілейованого доступу користувачів інформаційної системи організації

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1 Мета, завдання та цілі привілейованого доступу інформаційної системи організації

Привілейований доступ — це обліковий запис користувача, який має більше привілеїв, ніж звичайні користувачі. Привілейовані облікові записи можуть, наприклад, мати змогу встановлювати або видаляти програмне забезпечення, оновлювати операційну систему або змінювати конфігурації системи чи програми. Вони також можуть мати доступ до файлів, які зазвичай недоступні звичайним користувачам [1].

Привілейовані облікові записи зазвичай пов’язані з ролями в організації. Приклади включають IT-адміністраторів, груп безпеки, експертів служби підтримки, сторонніх підрядників, власників додатків, адміністраторів баз даних, облікових записів операційних систем і служб тощо.

Привілейованим обліковим записом також може бути обліковий запис «машина-машина» (M2M) або «прикладна програма-програма» (A2A), яка виконує автоматичні операції без участі людини. Типові приклади включають автоматизовані платіжні транзакції, розумне відстеження активів в організації, автоматизовану обробку даних або щоденне резервне копіювання критично важливих корпоративних даних[1].

Оскільки привілейовані облікові записи завжди надають доступ до інформації або цілей, які є цінними або критичними для операцій бізнесу, вони вимагають особливої уваги та управління аудитом.

Існує багато типів привілейованих облікових записів:

Облікові записи *root* і адміністратора зазвичай використовуються для встановлення та видалення програмного забезпечення та зміни конфігурацій. Вони

надають дуже широкі та найвищі привілеї доступу до певних серверів або баз даних і також належним чином називаються обліковими записами суперкористувача.

У Windows облікові записи адміністратора – це облікові записи користувачів, які використовуються для керування комп'ютером, доменом або всією IT-інфраструктурою підприємства.

Облікові записи адміністратора часто використовуються на автономних комп'ютерах і в невеликих середовищах. Однак будь-якого користувача Windows можна зробити адміністратором, додавши його до відповідної групи – *Administrator*.

Поширені підтипи облікових записів адміністратора включають локального адміністратора та адміністратора домену .

Облікові записи адміністратора домену надають повний доступ і контроль над доменом Active Directory (AD). Ці облікові записи особливо захищені та небезпечні, оскільки вони дають контроль над усіма контролерами домену, робочими станціями домену та серверами-учасниками домену. Вони дозволяють змінювати конфігурацію Active Directory або будь-який вміст, що зберігається в Active Directory. Це включає створення нових користувачів, видалення користувачів і зміну їхніх дозволів.

Адміністратор домену – це свого роду *Administrator* облікового запису.

Облікові записи локального адміністратора — це облікові записи користувачів, які можуть керувати локальним комп'ютером у Windows. Як правило, локальний адміністратор може робити будь-що з локальним комп'ютером, але не може змінювати інформацію в активному каталозі для інших комп'ютерів та інших користувачів.

Обліковий запис локального адміністратора часто називають адміністратором, але будь-який користувач може стати локальним адміністратором, додавши його до групи локальних адміністраторів.

Облікові записи служб використовуються для запуску процесів, таких як веб-сервери, сервери баз даних і сервери програм. Сервісні облікові записи також можна створювати лише для володіння даними та конфігураційними файлами.

Службові облікові записи не призначені для використання людьми, за винятком виконання адміністративних операцій.

Облікові записи програми пов’язані з певним прикладним програмним забезпеченням і зазвичай адмініструють, налаштовують або керують доступом до прикладного програмного забезпечення. Облікові записи програм дозволяють взаємодіяти між програмами та зазвичай запускаються автоматично без участі людини. Винятком із правила є завдання з обслуговування, які виконуються привілейованими користувачами.

Системні облікові записи створюються операційною системою під час встановлення та використовуються для запуску компонентів операційної системи та володіння пов’язаними файлами.

Системні облікові записи часто мають попередньо визначені ідентифікатори користувачів. Приклади системних облікових записів включають обліковий запис root у Linux.

Різниця між системними обліковими записами та обліковими записами служби іноді розмита. Багато системних облікових записів запускають процеси операційної системи, і в цьому відношенні нагадують облікові записи служби. До деяких системних облікових записів, наприклад, також входять системні адміністратори *root.*

Управління привілейованим доступом (PAM) відноситься до набору процесів і інструментів для контролю, моніторингу та аудиту привілейованих облікових записів і доступу. Традиційні рішення PAM зазвичай базуються на сховищах паролів і ротації паролів, тоді як сучасні системи нового покоління взагалі уникають паролів.

1.2. Аналіз проблеми несанкціонованого доступу до привілейованих даних інформаційної системи організації

У секторі безпеки, необхідно звернути увагу на управління привілейованими обліковими записами або доступом до інформаційної системи організації.

За останні десятиріччя відбулося багато досягнень у сфері IT та програмного забезпечення. Однак кібербезпека або бізнес із забезпечення безпеки додатків і мереж постійно відстає.

Кібернетичні загрози вийшли за межі свого початку як зриви та рекламні трюки. Оскільки компанії та організації продовжують оцифровувати свої активи, хакери націлюються на фінансову вигоду, ставлячи на кону все більше й більше. Як наслідок, кібератаки стають все більш витонченими та поширеними. Не можна заперечувати важливість кібербезпеки на цьому ринку. За кілька десятиліть галузь зросла до колосальних розмірів доходів, отримавши на цьому шляху кілька мільярдних гігантів безпеки. Окрім того, що безпека надзвичайно швидко розвивається, вона також постійно змінюється в міру того, як вона наздоганяє прогрес IT та прикладних технологій. Тож однією з найцікавіших тенденцій у сфері кібербезпеки є розвиток привілейованого керування обліковими записами (PAM) який зростає, за допомогою якого забезпечується безпека мережі, периметру.

Стан керування привілейованим обліковим записом:

Керування привілейованими обліковими записами — це рівень IT-безпеки, який служить для захисту організацій від кібератак, які вже проникли на периметр мережі. По суті, після того, як хакер зламав мережу компанії, наступною метою є отримання доступу до облікових записів із все більшими привілейованими обліковими записами. Вищі облікові записи мають більший доступ до даних компанії.

Традиційно підприємства зосереджували більшість своїх зусиль безпеки на захисті периметра та запобіганні проникненню загроз у мережу. Однак кібер-зловмисники мають повну силу, щоб сіяти хаос, зламавши початковий брандмауер

мережі. Підприємствам вже недостатньо лише утримувати зловмисників від своїх мереж. Найбільш шкідливі кібератаки відбуваються, коли облікові дані привілейованого облікового запису скомпрометовані, що дозволяє іноземним зловмисникам мати такий самий рівень і ширину доступу, як будь-який адміністратор або внутрішній член компанії.

Провідні постачальники PAM, показують високий рівень доступу, наданий привілейованим обліковим записам.

Рис.1.1. Рівень доступу, наданий привілейованим обліковим записам

Помітні кібератаки на базу даних кредитних карток Target і клієнтську базу даних JP Morgan були здійснені через привілейовані облікові записи, приносячи все більше й більше розголосу цьому новому сектору. Через зростаючу складність і поширеність кібератак традиційні методи кібербезпеки потребують комплексного підходу до захисту привілейованих облікових записів.

Зниження значення периметра:

Зростання PAM відбувається разом із занепадом традиційної безпеки периметра. Значна частина витрат на IT припадає на безпеку периметра, який формує безпечний периметр навколо корпоративної мережі. Сюди входить ринок мережевих брандмауерів вартістю майже 8 мільярдів доларів, який очолюють такі великі гравці, як Palo Alto Networks (NYSE: PANW) і FireEye (NASDAQ: FEYE) та інші. Хоча безпека периметра відіграє важливу роль у багатьох сучасних стратегіях безпеки, у цьому підході є кілька проблемних областей.

1. Великі дані та хмара

Зі зростанням впровадження хмарних обчислень, мобільних пристроїв, соціальних мереж та Інтернету речей стає дедалі складніше правильно визначити межі корпоративної мережі. Традиційно дані проходили через одну мережу, надану компанією, тому вони були передбачуваними та контрольованими. Тепер периметр окреслюється особою, яка має доступ до пристрою. Зловмисники цілять в людину за клавіатурою. Співробітники або «інсайдери» можуть легко приносити мобільні пристрої та профілі соціальних мереж у приміщення та за його межі. Значна частина корпоративних даних більше не обмежена межами захищеної мережі.

Крім того, у міру того, як компанії збирають все більші обсяги даних, сам розмір мереж збільшився в рази, створюючи складнішу архітектуру та ще більше розмиваючи периметр.

2. Внутрішні загрози

Зовнішня частина периметра надійно захищена поточними рішеннями на ринку, але внутрішні компоненти мережі все ще залишаються незахищеними. Використання викрадених облікових даних для видавання себе за внутрішній обліковий запис стає популярним методом кіберзломів, зокрема резонансні порушення прав JP Morgan (NYSE: JPM) і Sony (NYSE: SNE), обидва пов’язані з імітацією привілейованих облікових записів.

Оскільки кібератаки стають все більш інтенсивними та всеосяжними, компанії визнають, що традиційних рішень безпеки периметра недостатньо для захисту від

прогресивних загроз. У результаті компанії все більше інвестують у внутрішню безпеку в центрі обробки даних, щоб захистити внутрішні частини своїх мереж. У найближчі кілька років управління привілейованими обліковими записами стане однією з найбільш значних сфер витрат у сфері кібербезпеки. [2]

Крім кібервтоми, підприємства стикаються з проблемою підтримки привілейованого доступу в актуальному стані, особливо коли ролі співробітників змінюються або коли вони залишають організацію. Невиконання цього може призвести до фінансових втрат для кількох організацій, коли привілейовані облікові записи згодом було зламано та зловживано. Сервісні облікові записи також викликають труднощі, оскільки раніше вони налаштовувалися зі статичним паролем, який не закінчується та ніколи не змінюється.

Тож всіма типами привілейованих облікових записів необхідно управляти та захищати їх . Розглянемо основні найбільш небезпечні привілейовані облікові записи, на які всі організації повинні звернути увагу та виявити, управляти та захистити, щоб зменшити ризики безпеки свого бізнесу.

До основних типів привілейованих облікових записів, які є небезпечними, якщо вони не захищені відносяться:

«Обліковий запис адміністратора домену»

Я вважаю цей тип привілейованого облікового запису є головним — обліковим записом, який може робити майже все. Так, обліковий запис адміністратора домену має ПОВНИЙ доступ і контроль над доменом AD. Ця група за замовчуванням є членом групи адміністраторів на всіх контролерах домену, усіх робочих станціях домену та всіх серверах-учасниках домену під час їх приєднання до домену. За замовчуванням обліковий запис адміністратора є членом цієї групи. [3]

Ці облікові записи мають бути максимально обмежені; доступ і використання цих облікових записів має бути надано виключно на основі «за вимогою» з додатковими засобами контролю безпеки, щоб запобігти несанкціонованому використанню. Вся діяльність має проходити повний аудит і моніторинг.

«Облікові записи служби домену»

Ці облікові записи об’єднують кілька систем і програм, щоб вони могли спілкуватися та отримувати доступ до необхідних ресурсів, як правило, для запуску звітів, доступу до баз даних або викликів API. Ці облікові записи, як правило, викликають проблеми, особливо під час зміни пароля, що майже в усіх ситуаціях порушує роботу програми(ів), доки обліковий запис не буде синхронізовано в середовищі. Ці складні моменти означають, що більшість організацій мають політику «не торкайтеся цього пароля» щодо цих облікових записів або мають детальні процедури щодо того, як з ними поводитися. Ці облікові записи зазвичай використовуються для рішень резервного копіювання, аналітичних рішень, розгортання програмного забезпечення та оновлення патчів безпеки.

«Облікові записи локального адміністратора»

Іноді називають забутим привілейованим обліковим записом — обліковим записом, який багато організацій просто надають усім співробітникам, і обліковим записом, який націлюють усі кіберзлочинці, щоб отримати доступ до дверей, дозволяючи їм виявити та оцінити безпеку та захист організації. Це головна причина надмірних привілеїв працівників.

Обліковий запис локального адміністратора за умовчанням є обліковим записом користувача для системного адміністратора. Кожен комп’ютер має обліковий запис адміністратора (SID S-1-5- домен -500, відображуване ім’я Administrator). Обліковий запис адміністратора – це перший обліковий запис, який створюється під час встановлення для всіх операційних систем Windows Server і клієнтських операційних систем Windows.

Для операційних систем Windows Server обліковий запис адміністратора надає користувачеві повний контроль над файлами, каталогами, службами та іншими ресурсами, які знаходяться під контролем локального сервера. Обліковий запис адміністратора можна використовувати для створення локальних користувачів і

призначення прав користувачів і дозволів контролю доступу. Обліковий запис адміністратора також можна використовувати для контролю над локальними ресурсами в будь-який час, просто змінивши права користувача та дозволи.

Обліковий запис адміністратора за замовчуванням не можна видалити або заблокувати, але його можна перейменувати або вимкнути». [3]

«Екстренні облікові записи»

Ці облікові записи зазвичай вимкнено за замовчуванням, доки не станеться критичний інцидент, після чого певним користувачам потрібен привілейований доступ для відновлення систем, служб або навіть реагування на кіберінциденти. Вони використовуються лише в екстрених ситуаціях (зазвичай відомих як «розбити скло»), коли звичайні послуги недоступні. Наприклад, під час кіберінциденту ці екстрені облікові записи використовуються для доступу до систем, щоб провести цифрову криміналістику та зменшити записи журналів. Їх також можна використовувати для обмеження зламаних облікових записів від постійного зловживання.

«Сервісні облікові записи»

Службові облікові записи зазвичай використовуються в операційних системах для виконання додатків або програм у контексті системних облікових записів (облікових записів із високим рівнем привілейованих облікових записів без будь-якого пароля) або спеціального облікового запису користувача, який зазвичай створюється вручну або під час встановлення програмного забезпечення. В Unix і Linux вони часто відомі як init або inetd і також можуть запускати програми. Обліковим записам служб зазвичай не дозволяється входити в системи, однак вони, як правило, мають паролі, які ніколи не змінюються, і термін дії цих облікових записів не закінчується. Облікові записи зазвичай піддаються зловживанням з боку кіберзлочинців, які знаходять способи зламати їх, щоб вони могли запускати власні двійкові файли з підвищеними привілеями, дозволяючи зловмиснику віддалений доступ.

«Облікові записи програми»

Облікові записи програми регулярно використовуються, щоб гарантувати, що програма має доступ до ресурсів, необхідних для функціонування, таких як бази даних, мережа, автоматизовані завдання (наприклад, розгортання програмного забезпечення), автоматичні оновлення та можливість вносити зміни в конфігурацію. Ці облікові записи зазвичай зберігають паролі у файлах конфігурації або іноді використовують локальні або службові облікові записи для отримання необхідного доступу. Облікові записи програм також є мішенню для кіберзлочинців, оскільки їх можна легко зловживати, використовуючи відомі вразливості, які дозволяють зловмисникам отримати віддалений доступ, змінювати двійкові файли системи або підвищувати стандартні облікові записи до привілейованих, щоб вони могли пересуватися по мережі. Більшість організацій не вміють належним чином виправляти програми, тому зловмисники можуть занадто часто зловживати цими вразливими місцями.

«Облікові записи користувачів із привілейованими даними»

Це, мабуть, найнебезпечніший привілейований доступ з усіх. Так, цей обліковий запис є стандартним обліковим записом користувача, але має ДОСТУП до КОНФІДЕНЦІЙНИХ ПРИВІЛЕГОВОВАНИХ ДАНИХ. Подумайте про лікаря, який має доступ до даних пацієнтів, або про бухгалтера, який має доступ до фінансової звітності. Хоча ці облікові записи є звичайними, все залежить від того, до чого вони мають доступ . Облікові записи користувачів із привілейованими даними іноді не контролюються та не захищаються, як привілейовані облікові записи, і безпека зосереджена на програмі, де зберігаються дані, але не завжди. Організації повинні виконати оцінку ризику даних, щоб виявити привілейовані дані та захистити ВСІ стандартні облікові записи, які мають доступ до конфіденційних даних.

Інші типи привілейованих облікових записів:

– Облікові записи, які використовуються для доступу до рішень безпеки.
– Облікові записи Wi-Fi.

– Апаратні облікові записи, такі як BIOS і vPro.
– Облікові записи привілейованих користувачів.
– Мережеве обладнання.
– Облікові записи брандмауера.
– і навіть спільні привілейовані облікові записи.

1.3. Аналіз існуючих технологій управління привілейованим доступом до інформаційної системи організації

Чітке розуміння про основні технології управління привілейованим доступом до інформаційної системи організації надає магічний квадрант Gartner, звіт якого опубліковано 19 липня 2022 р. [4]

Виходячи зі звіту, можна сказати, що хоча основні продукти PAM продовжують залишатися важливими інструментами безпеки, зміна попиту на ринку зробила новий акцент на хмарі, від доставки інструментів PAM SaaS до розширення функціональності для хмарної безпеки в інструментах PAM, включаючи управління секретами та CIEM.

Інструменти управління привілейованим доступом (PAM) використовуються для зменшення ризику привілейованого доступу. Тобто це відноситься до облікових записів, облікових даних та операції, які пропонують підвищений (або «привілейований») рівень доступу. Інструменти PAM використовуються машинами (програмним забезпеченням) і людьми, які адмініструють або налаштовують IT-інфраструктуру або інформаційну систему організацій. Рішення PAM можна розгорнути як локальне програмне забезпечення, SaaS або апаратне забезпечення.

Основні можливості PAM включають:

– Виявлення привілейованих облікових записів у багатьох системах, інфраструктурі та програмах.
– Керування обліковими даними для привілейованих облікових записів.

– Сховище облікових даних і контроль доступу до привілейованих облікових записів.

– Створення сеансу, керування, моніторинг і запис для інтерактивного привілейованого доступу.

Додаткові можливості PAM включають:

– Делегування доступу до привілейованих облікових записів;

– Контрольоване підвищення команд;

– Управління секретами програм, сервісів і пристроїв;

– Автоматизація привілейованих завдань;

– Віддалений привілейований доступ для працівників та зовнішніх користувачів;

– Управління правами доступу до хмарної інфраструктури (CIEM).

Gartner визначає чотири різні категорії інструментів для інструментів PAM :

1. Керування привілейованим обліковим записом і сеансом (PASM): привілейовані облікові записи захищені шляхом зберігання їхніх облікових даних. Потім доступ до цих облікових записів надається користувачам, службам і програмам через інструмент PAM. Функції керування привілейованими сеансами (PSM) встановлюють сеанси, як правило, із введенням облікових даних і записом повного сеансу. Паролі та інші облікові дані , такі як сертифікати та токени для привілейованих облікових записів, активно керуються (наприклад, змінюються через визначені проміжки часу або після виникнення певних подій). Рішення PASM додатково можуть забезпечувати керування паролями від програми до програми (AAPM) і/або без встановлення функції віддаленого привілейованого доступу для зовнішнього IT-персоналу та третіх сторін, яким не потрібно VPN.

2. Підвищені повноваження і управління делегуванням (PEDM): агенти на основі хосту в керованій системі надають певні привілеї користувачам, які ввійшли в систему. Інструменти PEDM забезпечують керування командами на основі хоста (фільтрування), елементи керування дозволом/забороною/ізоляцією додатків та/або

підвищення привілеїв, що дозволяє запускати певні процеси з вищим рівнем привілеїв. Інструменти PEDM мають виконуватися у фактичній операційній системі (на рівні ядра чи процесу). Управління командами за допомогою фільтрації протоколу явно виключено з цього визначення, оскільки точка керування менш надійна. Інструменти PEDM також можуть надавати елементи управління додатками та функції моніторингу цілісності файлів. Інструменти PEDM часто є обов'язковою вимогою для регульованих галузей і там, де передбачено дотримання PCI-DSS, SOX та інших регулятивних і фінансових засобів контролю.

3. Управління секретами: облікові дані (наприклад, паролі, маркери OAuth і ключі SSH) і секрети для програмного забезпечення та машин, які управляються програмно, зберігаються та витягуються через API та SDK. Довіра встановлюється та підтримується з метою обміну секретами та керування авторизаціями та пов'язаними функціями між різними нелюдськими об'єктами, такими як машини, контейнери, програми, служби, сценарії, процеси та конвеєри DevSecOps. Керування секретами часто використовується в динамічних і гнучких середовищах, таких як IaaS, PaaS і платформи керування контейнерами. Продукти керування секретами також можуть надавати AAPM.

4. CIEM: пропозиції CIEM — це спеціалізовані SaaS-рішення, орієнтовані на ідентифікацію, які зосереджені на управлінні ризиками доступу до хмари за допомогою контролю часу адміністрування, що регулює права доступу в гібридних і багатохмарних IaaS. Вони зазвичай використовують аналітику, машинне навчання (ML) або інші методи для виявлення аномалій у правах облікових записів, як-от накопичення привілеїв або неактивні та непотрібні права. CIEM ідеально забезпечує виправлення надмірних дозволів і застосування підходів із найменшими привілеями в хмарних інфраструктурах.

Рис 1.2. Рішення PAM [4]

Розглянемо переваги та недоліки лідерів рішень за магічним квадрантом Gartner. [4]

Рішення ARCON

ARCON є лідером у цьому магічному квадранті. Функціональність PASM ARCON надається продуктом ARCON/PAM (підприємство), а функціональність PEDM — продуктом ARCON/EPM. ARCON пропонує основні функції керування секретами за допомогою інструменту PAM від програми до програми, інтерфейсів до

інструментів інфраструктури Dev-Ops і CIEM. ARCON може надавати функціональні можливості PASM через пристрій, програмне забезпечення (самокероване) або SaaS. ARCON в основному зосереджена на клієнтах в Азіатсько-Тихоокеанському регіоні та EMEA. ARCON є одним із небагатьох постачальників PAM, які зосереджені на операційних технологіях, і цього року додали функцію офлайн-сховища для вирішення випадків використання критичної інфраструктури з розривом повітря.

Переваги

ARCON отримала переваги завдяки додаванню можливостей продукту протягом останнього року, особливо в управлінні секретами, CIEM і функціях «точно вчасно».

Особливість ARCON покладається на агентів і клієнтські інструменти для найкращої взаємодії з користувачем. Альтернативою є використання плагіна для веб-переглядача, однак функціональність тоді не така бездоганна, як у інших рішень. Недолік - Arcon має обмежену кількість готових інтеграцій для суміжних технологій.

BeyondTrust

BeyondTrust є лідером у цьому магічному квадранті. У 2018 році чотири взаємодоповнюючі компанії PAM об’єдналися, щоб створити комплексний набір функцій PAM, включаючи зрілий продукт віддаленого доступу під назвою Bomgar. Послуги PASM надаються за допомогою Password Safe (SaaS або програмного забезпечення) з функціональністю PEDM, яка надається за допомогою інструментів керування привілеями та AD. Керування секретами забезпечує DevOps Secret Safe, а BeyondTrust також пропонує функціональні можливості CIEM за допомогою інструменту Cloud Privilege Broker. BeyondTrust представив покращену консолідовану платформу SaaS і функціональність CIEM.

Переваги

Продукт: BeyondTrust пропонує комплексний PEDM на основі агентів Windows/Linux/UNIX/macOS , журнал привілейованого доступу, звітування та аудит,

аналітику та реагування. Він сильний завдяки своїй продуктивності та масштабованості, доступності та можливостям відновлення.

Недоліки

Для керування секретами BeyondTrust отримав найнижчий бал за загальну функціональність серед усіх постачальників, які пропонують окремий продукт для керування секретами, без підтримки власних механізмів автентифікації та інтеграції з технологіями DevOps. Оцінки керування привілейованим сеансом також були низькими.

Broadcom (Symantec)

Broadcom (Symantec) є нішевим гравцем у цьому магічному квадранті. Symantec — це велика компанія-виробник програмного забезпечення, яка пропонує продукт PAM, який неодноразово ребрендингувався та тепер пропонується під брендом Symantec. Її продукт PAM доступний лише у варіантах доставки програмного та апаратного забезпечення. Symantec пропонує функції PASM і PEDM у продукті Symantec Privileged Access Management. Він також пропонує менеджер між програмами та інструмент аналітики, але нічого не пропонується щодо керування секретами чи CIEM, хоча керування секретами є дорожньою картою. Symantec має значну кількість клієнтів у NA, EMEA та APAC, і цього року компанія представила новий утилітарний пристрій, віртуальний пристрій для свого продукту PAM .

Переваги

Symantec пропонує дуже конкурентоспроможний продукт PEDM для клієнтів Windows, Linux/UNIX і мейнфреймів. Продуктивність і масштабованість, доступність і можливості відновлення є сильними для PASM, включаючи відмінні функції кластеризації та високої доступності, які підтримують додавання вузлів без необхідності відключати кластер. Для автоматизації та інтеграції суміжної системи Symantec підтримує лише SiteMinder для попередньо створених інтеграцій для SSO, він підтримує SSO на основі стандартів і пропонує хороший набір інтеграцій із

суміжними технологіями, такими як IGA та ITSM, а також як інтеграції на основі API, CLI та Java.

Недоліки

Для комплексного керування обліковими даними облікового запису служби Symantec покладається на свою платформу Custom Connector Framework, але це означає, що клієнтам іноді доводиться розробляти спеціальні лінії з'єднування, тоді як інші постачальники пропонують готові з'єднувачі. Керування обліковими даними привілеїв і JIT PAM також були менш зрілими порівняно з ринком.

CyberArk

CyberArk є лідером у цьому магічному квадранті. CyberArk запатентувала технологію сховища понад 22 роки тому та була першим постачальником PAM, який представив у своєму продукті як керування секретами, так і функціональність CIEM. CyberArk пропонує функціональні можливості PASM із диспетчером привілейованого доступу, функціональні можливості PEDM (SaaS або програмне забезпечення) з інструментом Endpoint Privileged Manager, керування секретами та керування додатками за допомогою диспетчера секретів і функціональність CIEM із диспетчером хмарних прав. Він також пропонує віддалений інструмент PAM під назвою Vendor Privileged Access Manager. CyberArk має значну клієнтську базу в усіх основних ринкових регіонах і цього року запровадив офлайн-доступ до сховищ для закритих середовищ.

Переваги

Продукт: у CyberArk є велика партнерська екосистема, яка надала багато з'єднувачів та інтеграцій із суміжними технологіями, такими як ITSM та інструменти управління та адміністрування ідентифікаційної інформації (IGA). Пропозиція CyberArk PAM є дуже конкурентоспроможною, пропонуючи одні з найдосконаліших можливостей на ринку, особливо PASM та його функції керування секретами, а також керування привілейованим доступом, керування обліковими даними, журналювання та звітування, інтеграцію та автоматизацію суміжних технологій, а також CIEM.

Недоліки

Функції керування безперервністю та високої доступності CyberArk для його програмного забезпечення, наданих (самокерованих) інструментів PASM залишаються складними для налаштування та експлуатації. Аварійне відновлення, особливо підтримка відновлення після збоїв, є крихким, покладається на ручні процеси та протягом тривалого часу є джерелом скарг клієнтів.

Delinea

Delinea є лідером у цьому магічному квадранті. Delinea — це нова компанія, яка представляє поєднання двох колишніх компаній (Centrify і Thycotic), які були лідерами минулорічного магічного квадранту PAM. Функції PASM тепер охоплені продуктом Secret Server від Thycotic. PEDM покривається Privilege Manager від Thycotic. Сервер PAM, продукти служби автентифікації та інструменти AD Bridging від Centrify. Обидва ці продукти доступні як програмне забезпечення або SaaS. DevOps Secrets Vault — це продукт для керування секретами. Наразі можливості CIEM не пропонуються, але вони плануються. Delinea випустила оновлений функціонал для консолідованої служби SaaS. Сильні сторони

Переваги

Delinea досягла прогресу у своїх можливостях керування секретами завдяки інтеграції додаткових інструментів розробника. Delinea також отримала високі оцінки в управлінні життєвим циклом облікових записів служб (хоча для цього потрібно придбати окремий інструмент) і в управлінні привілейованим доступом до баз даних. Delinea отримала хороші оцінки за виявлення облікових записів і адаптацію, за функціональність PEDM для Windows і UNIX/Linux/macOS. (

Недоліки

Продукт: в управлінні сеансами RDP Delinea відсутній власний запис без агентів, функція, яка досить поширена серед більшості конкурентів. Секретний сервер відстає в керуванні обліковим записом служби та обліковими даними, і особливо чутливий у локальних системах, які не підключені постійно.

Hitachi ID

Hitachi ID є нішевим гравцем у цьому магічному квадранті. Hitachi ID пропонує функції PASM через продукт Bravura Privilege, програмний інструмент PAM. Hitachi ID не пропонує функціональність PEDM (хоча PEDM є в його дорожній карті) або функціональність CIEM.

Переваги

Bravura Privilege має потужні можливості для виявлення та керування обліковими даними, включаючи готові з'єднувачі для облікових записів служб, а також відмінні можливості для керування обліковими даними на кінцевих точках, які не підключені постійно.

Bravura Privilege має чудові готові можливості для аварійного відновлення та відновлення після відмови, які добре перевірені та прості в налаштуванні.

Hitachi ID має багато інтеграцій із суміжними технологіями, що використовуються з PAM, такими як керування IT-послугами, RPA та CMDB.

Hitachi ID має високопродуктивні та настроювані функції автоматизації в усіх своїх пропозиціях PAM, які добре перевірені та надійні.

Недоліки

Hitachi ID пропонує керування паролями від програми до програми на основі агента з кількома унікальними підходами до уникнення збереження секретів у стані спокою, але наразі не має подібних можливостей керування секретами. Крім того, Bravura Privilege підтримує лише локальний запис сеансу та не надає початкових проксі-серверів сеансу чи можливостей фільтрації.

В результаті аналізу існуючих технологій для подальшого дослідження обраємо Privilege Manager рішення Delinea, яке досягло прогресу у своїх можливостях керування секретами, а також отримала високі оцінки в управлінні життєвим циклом облікових записів служб.

2 МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ ПРИВІЛЕЙОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Моделі та методи контролю доступу

Кібербезпека з найменшими привілеями забезпечує застосування моделі безпеки на основі ризику з нульовою довірою, згідно з якою після перевірки користувача доступ користувача обмежується лише тим, що необхідно для виконання конкретного завдання чи роботи. Якщо будь-яка дія користувача потребує більшого доступу, ніж надано правилами політики, дозволи на підвищення привілеїв суворо контролюються та відстежуються. Будучи простим доступом відповідно до концепції, при забезпеченні найменших привілеїв в IT-середовищах може бути дуже складним і включати сотні, якщо не тисячі, користувачів, програм і служб, яким потрібен доступ до привілейованих дозволів.

Нульова довіра передбачає, що будь-який користувач або система, яка отримує доступ до мережі, служб, програм, даних або систем, починає з нульовою довірою. Щоб отримати авторизований доступ, потенційний користувач має заслужити довіру шляхом перевірки. Наприклад, для перевірки може знадобитися двофакторна автентифікація. У цьому випадку користувач надає пароль, але потім потрібно зробити додатковий крок за допомогою програми автентифікації. Коли нові пристрої вводяться в мережу — і перш ніж вони отримають доступ до будь-яких ресурсів — вони повинні спочатку ідентифікувати та перевірити себе на основі різних засобів контролю безпеки. Чим чутливіші ресурси, до яких потрібно отримати доступ, тим більше засобів контролю безпеки вони повинні задовольняти.

Кібербезпека завжди повинна починатися з нульової довіри, гарантуючи, що дозволено лише авторизований доступ. Після підтвердження особи користувачі можуть бути класифіковані відповідно до доступу, необхідного для виконання своїх завдань.

Динамічна класифікація довіри

Класифікації довіри та прийнятного ризику кібербезпеки мають бути динамічними. Це означає, що вам потрібно створити політики або правила в масштабах підприємства для ідентифікаторів, служб, програм, даних і систем. Наприклад, ви можете вибрати «завжди перевіряти» та «завжди моніторити» для ідентифікаційних даних сторонніх постачальників або підрядників. Внутрішні класифікації співробітників будуть адаптивними на основі чутливості даних, до яких здійснюється доступ.

Політика завжди перевіряти потребуватиме облікових даних і багатофакторної автентифікації, тоді як політика постійного моніторингу здійснюватиме аудит і запис усіх дій.

З*апобігання експлуатації надпривілейованих користувачів*

Багато разів компанії ненавмисно надають своїм співробітникам занадто широкий доступ до інформації про облікові записи. Цей недогляд призводить до надто привілейованих користувачів і може призвести до порушень у вашій компанії. Візьміть Сару, наприклад, яка є працівником виробничої компанії. Щоб легко виконувати свою роботу, вона отримала ноутбук із правами облікового запису локального адміністратора. По суті, обліковий запис локального адміністратора дає їй відносно необмежений доступ до запуску програм, навіть якщо вона може не знати про це. Вона щойно стала надпривілейованим користувачем.

Одного дня Сара отримує електронний лист із вкладеним документом, який виглядає як законний запит від генерального директора компанії. Вона клацає вкладений файл і, сама того не розуміючи, завантажує шкідливе програмне

забезпечення, яке запускає процеси, які перехоплюють її ідентифікатор користувача та пароль.

Оскільки комп'ютер Сари має права локального адміністратора, зловмисному програмному забезпеченню вдалося відредагувати реєстр комп'ютера, дозволяючи зловмисному програмному забезпеченню — і кіберзлочинцю — зберігатися на комп'ютері Сари. Сари і не розуміє, що зловмисне програмне забезпечення також захопило хеші облікових даних Сари, що дозволило йому перетинати інші зони IT-мережі її компанії. Зловмисне програмне забезпечення замітає свої сліди, змінюючи журнали аудиту. Ніхто не знає, що кіберзлочинець знаходиться всередині мережі. І все це відбувається завдяки тому, що відомо як захоплення прав локального адміністратора — скомпрометований привілейований обліковий запис у результаті використання надпривілейованого користувача.

Інші класифікації такі:

» Служби та програми можна класифікувати за конфіденційністю даних, до яких служба або програма має доступ.

Наприклад, чи містять вони конфіденційну інформацію, таку як дані кредитної картки чи медичні записи?

» Пристрої можна класифікувати як персональні пристрої співробітників і пристрої підрядників, а також пристрої, які належать і керуються компаніями. Особисті пристрої або пристрої підрядників повинні належати до класифікації «ніколи не надійних», оскільки ви ніколи не знаєте, які програми чи зловмисне програмне забезпечення існують на цих пристроях для використання можливостей. Таким чином, сегментуйте мережі, щоб відрізнити ненадійні мережі, наприклад персональні пристрої або пристрої підрядників, від надійних мереж, які можуть підключатися лише до відомих керованих корпоративних систем.

Застосування найменших привілеїв

Застосування найменших привілеїв має два аспекти:

» Конфіденційність: коли користувач входить, він може бачити лише те, до чого йому дозволено доступ.

» Безпека: на основі певного привілейованого доступу користувач має обмеження на те, які програми/завдання він може запускати.

Застосування мінімальних привілеїв зазвичай починається з видалення локальних адміністративних привілеїв на кінцевих точках, таких як ноутбуки користувачів або мобільні пристрої, щоб ви могли зменшити вразливість атак і запобігти більшості атак. Найменший привілей ефективний для зменшення основних проблем із керуванням виправленнями. Застосування найменшої безпеки привілеїв може допомогти усунути понад 90 відсотків виправлень Microsoft Windows, оскільки для використання більшості вразливостей потрібні права адміністратора.

АНАЛОГІЯ ДОСТУПУ В ГОТЕЛЬ

Реалізація нульової довіри з найменшими привілеями може бути легшою для розуміння, якщо виражати її через аналогію з доступом до готелю. Деякі системи кібербезпеки перевіряють користувачів співробітників на вході в лобі готелю. Після того, як особу перевірено, вона фактично отримує головний ключ з доступом до всіх зон і номерів готелю. Він може вільно ходити по коридорах готелю і заходити в будь-яку кімнату, навіть якщо вона замкнена. Ніхто не буде оскаржувати його дії, і йому не потрібно, щоб хтось допомагав йому отримати доступ. Він є користувачем із надлишковими правами.

Однак, коли застосовано найменший привілей, після перевірки особи користувач отримує ключ, який дозволяє йому лише в певну кімнату та/або на певний поверх. А коли найменші привілеї поєднуються з контролем додатків, особа може увійти в кімнату, але її дії обмежені, коли вона в кімнаті. Він, наприклад, може

відкрити кран у ванній, але не відкрити вікно. Якщо він спробує відкрити вікно, спрацює сигналізація, і охорона готелю дослідить потенційну загрозу безпеці.

Уявіть собі, що ви керуєте тисячами людей, які заходять у готель для ведення бізнесу. Перевірка особи у фойє може здатися логічною, але коли користувач увійшов, надати йому вільний доступ до кожної кімнати та частини готелю є надзвичайно ризикованим. У той же час ви не хочете, щоб користувачі були настільки обмежені в тому, куди вони можуть ходити і що вони можуть робити, щоб обмеження не дозволяли їм завершити свою роботу.

Відповідність вимогам

Багато вимог і нормативних актів вимагають суворого контролю безпеки під час використання привілейованого доступу. Організаціям, які надають кінцевим користувачам занадто багато привілеїв, завжди буде важко задовольнити більшість вимог відповідності. І коли вони застосовують суворий контроль для дотримання правил, вони можуть негативно вплинути на продуктивність користувача. Таким чином, дуже важливо створити стратегію найменших привілеїв, яка б обмежувала привілеї кінцевих користувачів, не перешкоджаючи співробітникам виконувати завдання, необхідні для успішного повноцінного виконання своєї роботи.

Більшість організацій переходять на хмарні технології, контроль доступу стає дедалі складнішим, оскільки потрібні як локальні, так і хмарні рішення. Незалежно від того, чи розташовані вони по всьому світу віддалено чи на місці, працівникам потрібен доступ для виконання своєї роботи. Коли працівники не мають відповідного рівня доступу для читання та/або зміни інформації, такої як документи, слайди та інші файли на мережевому диску, бізнес ускладнюється, а результати можуть бути кардинальними.

Це може статися в найнезручніший момент, і користувачам швидко потрібен системний адміністратор, щоб надати відповідні рівні привілеїв.

Зазвичай співробітники та користувачі цікавляться, чому вони не можуть просто отримати загальний доступ до інформації в папці, щоб вони могли сортувати елементи

та знаходити те, що їм потрібно. На жаль для користувачів, відповідь системного адміністратора може бути такою: «Вибачте, вам потрібно подати заявку, перш ніж ми зможемо надати вам потрібний вам рівень доступу».[6]

Ця відповідь ще більше розчаровує, оскільки користувачеві потрібно продовжити виконання свого завдання, і все, що йому потрібно, це доступ до однієї папки. І що тепер? Як би незручно це було, існують причини, чому контроль доступу вступає в гру для такого сценарію, зокрема з точки зору кібербезпеки. Для контролю доступу існують 4 моделі контролю доступу. Опишемо методи логічного контролю доступу та поясню різні типи контролю фізичного доступу. [6]

Контроль доступу – це процес:

– визначення особи, яка виконує певну роботу;

– автентифікація користувачів, з огляду на їхню ідентифікацію;

– надання людині лише ключа від дверей чи комп’ютера, до якого їй потрібен доступ, і нічого більше.

В кібербезпеці це можна розглядати як:

– надання індивідуального дозволу на доступ до мережі за допомогою імені користувача та пароля;

– дозволяти користувачам отримати доступ до файлів, комп’ютерів або іншого необхідного апаратного чи програмного забезпечення;

– гарантувати, що користувачі мають належний рівень дозволу для виконання своєї роботи. [6]

Отже, як надати належний рівень дозволу користувачам, щоб вони могли виконувати свої обов’язки? Ось тут і з’являються моделі контролю доступу.

Моделі контролю доступу мають чотири види:

1. Обов'язковий контроль доступу (MAC)
2. Контроль доступу на основі ролей (RBAC)
3. Дискреційний контроль доступу (DAC)
4. Керування доступом на основі правил (RBAC або RB-RBAC)

1. Модель обов'язкового контролю доступу, або MAC, надає управління контролем доступу лише власнику та зберігачу. Це означає, що кінцевий користувач не може контролювати будь-які налаштування, які надають будь-які привілеї будь-кому. Зараз існує дві моделі безпеки, пов'язані з MAC: Biba та Bell-LaPadula.

Модель Біба зосереджена на цілісності інформації, тоді як модель Белла-Ла Падули зосереджена на конфіденційності інформації. Biba — це налаштування, за яким користувач із низьким рівнем доступу може читати інформацію вищого рівня (так званий «зчитування»), а користувач із високим рівнем доступу може писати з нижчим рівнем доступу (так званий «запис»). Модель Biba зазвичай використовується в компаніях, де співробітники нижчого рівня можуть читати інформацію вищого рівня, а керівники можуть писати, щоб повідомити співробітників нижчого рівня.

Белл-Ла Падула , з іншого боку, — це налаштування, за якого користувач на вищому рівні (тобто Цілком таємно) може писати лише на цьому рівні, але не нижче (так званий «запис»), але також може читати на нижчих рівнях (так званий «прочитай»). Bell-LaPadula був розроблений для урядових та/або військових цілей, де якщо хтось не має належного рівня допуску та не потребує знати певну інформацію, він не має жодного діла до інформації.

Свого часу MAC асоціювався з системою нумерації, яка призначала номер рівня для файлів і номер рівня для співробітників. Ця система створена так, що якщо файл (тобто myfile.ppt) має рівень 400, інший файл (тобто yourfile.docx) має рівень 600, а працівник має рівень 500, працівник не зможе отримати доступ до «yourfile». .docx" через вищий рівень (600), пов'язаний із файлом.

MAC — це найвищий рівень контролю доступу, який використовується у військових та/або державних установах із використанням класифікацій «Секретно», «Таємно» та «Несекретно» замість системи нумерації, згаданої раніше.

Рис 2.1. Модель обов'язкового контролю доступу MAC [6]

2. *Модель контролю доступу на основі ролей, або RBAC*, забезпечує контроль доступу на основі посади, яку особа займає в організації. Отже, замість того, щоб призначати Алісі дозволи як менеджеру безпеки, посада менеджера безпеки вже має призначені дозволи. По суті, Алісі просто потрібен доступ до профілю менеджера безпеки.

RBAC полегшує життя системному адміністратору організації. Велика проблема цієї моделі контролю доступу полягає в тому, що якщо Алісі потрібен доступ до інших файлів, має бути інший спосіб зробити це, оскільки ролі пов'язані лише з роллю.; інакше менеджери безпеки з інших організацій можуть отримати доступ до файлів, для яких вони не мають прав.

Рис 2.2. Модель контролю доступу на основі ролей, або RBAC [6]

3. *Модель дискреційного контролю доступу, або DAC*, є найменш обмежувальною моделлю порівняно з найбільш обмежувальною моделлю MAC. DAC дозволяє окремим особам повністю контролювати будь-які об’єкти, якими вони володіють, а також програми, пов’язані з цими об’єктами.

Це дає DAC дві основні слабкості. По-перше, це дає кінцевому користувачеві повний контроль для встановлення налаштувань рівня безпеки для інших користувачів, що може призвести до того, що користувачі матимуть вищі привілеї, ніж вони повинні. По-друге, що ще гірше, дозволи, які має кінцевий користувач, успадковуються в інших програмах, які він виконує. Це означає, що кінцевий користувач може запускати зловмисне програмне забезпечення, не підозрюючи про це, і зловмисне програмне забезпечення може скористатися привілеями потенційно високого рівня, якими володіє кінцевий користувач.

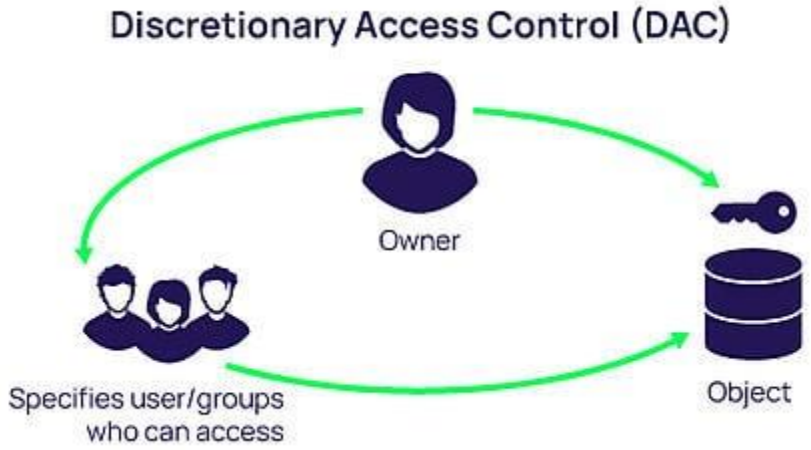

Рис.2.3. Модель дискреційного контролю доступу, або DAC [6]

4. Модель керування доступом на основі правил , також має абревіатуру RBAC або RB-RBAC. Контроль доступу на основі правил динамічно призначатиме ролі користувачам на основі критеріїв, визначених опікуном або системним адміністратором. Наприклад, якщо комусь дозволено доступ до файлів лише в певні години доби, контроль доступу на основі правил стане інструментом вибору.

Додаткові «правила» керування доступом на основі правил, які вимагають впровадження, можливо, доведеться «запрограмувати» системним адміністратором у формі коду, а не «поставити прапорець».

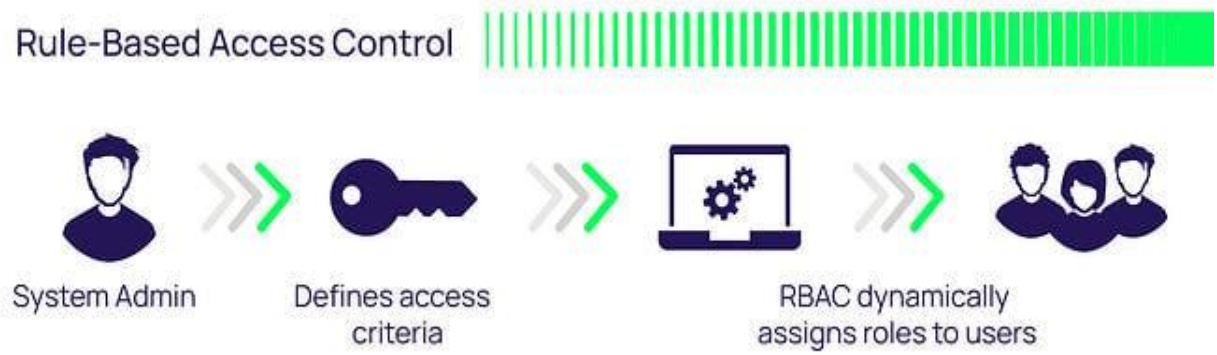

Рис.2.4. Модель управління доступом на основі правил RBAC [6]

Логічні методи контролю доступу

Логічний контроль доступу здійснюється за допомогою списків контролю доступу (ACL), групових політик, паролів і обмежень облікових записів. Розглянемо кожен із них, щоб побачити, як вони забезпечують контрольований доступ до ресурсів.

Списки контролю доступу (ACL) — це дозволи, додані до об’єкта (тобто файлу електронної таблиці), які система перевірятиме, щоб дозволити або заборонити контроль над цим об’єктом. Ці дозволи варіюються від повного контролю до лише читання та «доступ заборонено». Коли мова йде про різні операційні системи (тобто Windows®, Linux, Mac OS X®), записи в списках ACL називаються «запис керування доступом» або ACE і налаштовуються за допомогою чотирьох частин інформації: ідентифікатора безпеки (SID), маска доступу, прапорець для операцій, які можна виконувати з об’єктом, і інший набір прапорців для визначення успадкованих дозволів об’єкта. Отже, як можна побачити, ACL забезпечують детальний контроль доступу до об’єктів. Однак вони можуть стати громіздкими, коли зміни відбуваються часто, і потрібно керувати багатьма об’єктами.

Групові політики є частиною середовища Windows® і дозволяють централізоване керування доступом до мережі комп'ютерів за допомогою служб каталогів Microsoft під назвою Active Directory. Це усуває необхідність переходити до кожного комп'ютера та налаштовувати контроль доступу. Ці параметри зберігаються в об'єктах групової політики (GPO), що дає змогу системному адміністратору зручно налаштовувати параметри. Незважаючи на те, що це зручно, рішучий кіберзлочинець може обійти ці групові політики та погіршити життя системному адміністратору.

Паролі є найпоширенішим логічним контролем доступу. Іноді його називають логічним токеном (Ciampa, 2009). Паролі мають бути складними для злому, щоб забезпечити необхідний рівень контролю доступу. Якщо хтось робить пароль легким для вгадування або використовує слово зі словника, він може піддаватися атакам грубої сили, атакам за словником.

Пам'ятаючи про це, експерти сходяться на думці, що чим довший пароль, тим важче його зламати, за умови, що користувач пам'ятає його та використовує багато різних символів і неклавіатурних символів при його створенні. Використання цієї концепції також ускладнює кіберзлочинцям зламати пароль за допомогою райдужних таблиць.

Крім того, регулярне встановлення виправлень, видалення або відключення непотрібних облікових записів, захист BIOS паролем, забезпечення завантаження комп'ютера лише з жорсткого диска та тримання дверей на замку з комп'ютером за ними допоможуть забезпечити захист ваших паролів. Звичайно, не записувати пароль теж допоможе.

2.2. Життєвий цикл управління привілейованим доступом

Як і будь-який засіб IT-безпеки, призначений для захисту критичних інформаційні активи, управління та захист привілейованого доступу вимагає як

плану, так і постійної програми. Для цього необхідно визначити, які привілейовані облікові записи мають бути пріоритетними у вашій організації та гарантувати, що ті працівники, які використовують ці привілейовані облікові записи розуміють прийнятне використання та їх обов'язки.

На рисунку 2.1 показано життєвий цикл управління привілейованим доступом (PAM).

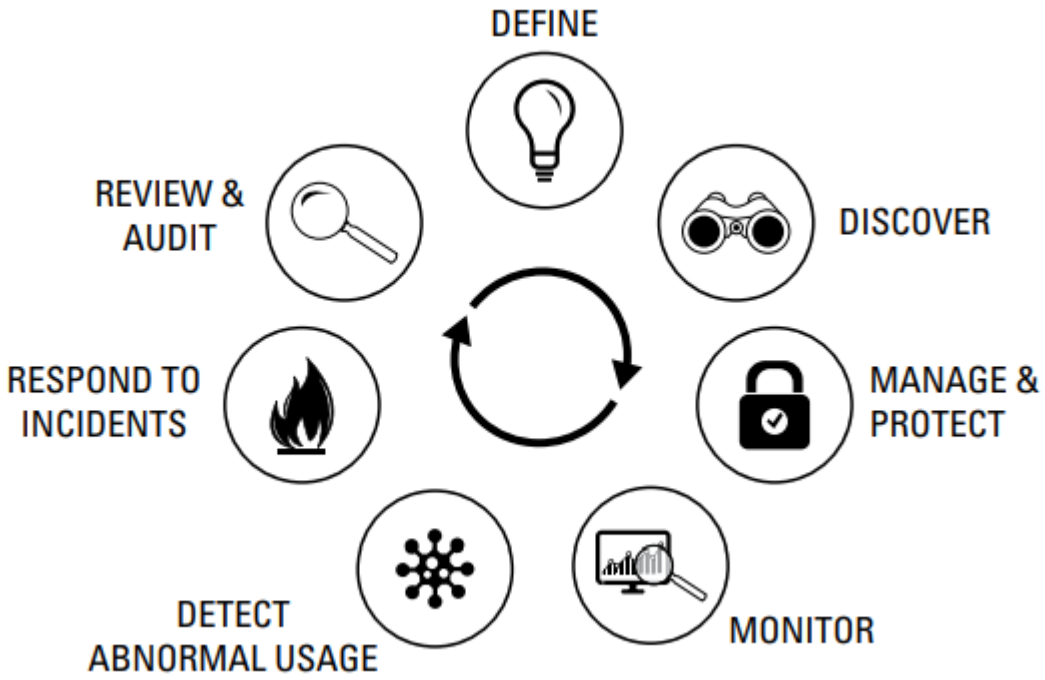

Рис. 2.1 Життєвий цикл управління привілейованим доступом

Такий циклічний підхід, необхідно включити до стратегії найменших привілеїв:

– Визначайте привілейований доступ і облікові записи;

– Постійно відкривайте привілейовані облікові записи;

– Керуйте, захищайте та контролюйте привілейовані облікові записи;

– Аудит і моніторинг використання розповсюдження, поширення або несанкціоноване використання суворо заборонено;

– Дослідіть незвичну поведінку;

– Реагуйте на інциденти;

– Перегляньте та оцініть контроль привілеїв доступу.

Вашим наступним кроком у реалізації стратегії найменших привілеїв буде визначення використання привілеїв у вашому середовищі на основі як ви визначаєте привілейований доступ:

– Хто має привілейований доступ;

– Коли він використовується;

– Для яких дій потрібен привілейований доступ;

– Які заходи безпеки слід застосовувати;

– Вимоги відповідності, пов’язані з привілейованим доступом.

Підхід життєвого циклу

Після визначення критичних активів призначте їх до привілейованих облікових записів, включення PAM і визначення використання привілеїв. Таким чином ваша організація буде готова до реалізації найменших привілеїв.

Використовуючи підхід життєвого циклу з найменшими привілеями, необхідно дотримуватись таких кроків:

» Виконайте пошук, щоб дізнатися, які кінцеві точки та локальні користувачі мають права адміністратора, які програми використовуються та якщо для їх запуску потрібні права адміністратора.

» Створіть білий список прийнятних довірених програм і процеси.

» Блокуйте відомі шкідливі файли за допомогою списку заборони.

» Керуйте невідомими областями за допомогою списку обмежень і автоматизованого робочого процесу, щоб дозволити запускати та блокувати схвалені програми.

» Встановіть контекстуальні політики, які відповідають оцінці ризику.

» Плануйте, щоб користувачі змінювали ролі або відділи.

» Не обмежуйтесь лише кінцевими точками, контрольованими доменом.

» Не забувайте про дочірні процеси.

» Інтегруйте робочий процес у наявні інструменти.

2.3. Архітектура привілейованого доступу

Архітектура привілейованого доступу повинна включати необхідну кількість компонентів, які виконують свої функції в реалізації технології привілейованого доступу організацій. Саме процес виконання функцій цих компонент PAM дозволить знизити ризики витоку інформації інформаційної системи організації. Розглянемо ці компоненти детально. (див. табл. 2.1). [4]

Таблиця 2.1.

Компоненти PAM та їх функції

Component ID	**Функції**
1. Полегшений протокол доступу до каталогу Identity Store (LDAP)	1. Репозиторій ідентифікаційних даних, спеціально зарезервований для привілейованих користувачів організації 2. Моніторинг та звітність про зміни облікового запису
2. MFA Multifactor Authentication	3. Додаткові можливості MFA для автентифікації користувача системи PAM 4. Журнали кожної спроби автентифікації
3. Інтерфейс користувача	5. Автентифікація входу та інтерактивний інтерфейс користувача-системи PAM, через який користувачі взаємодіють для встановлення робочих сеансів для кожної системи, якою вони адмініструють або до якої мають доступ для виконання своїх робочих функцій
4. Policy Management - Управління політикою	6. Корпоративні політики доступу та контролю для привілейованих користувачів, наприклад сеанси

	привілейованих користувачів, обмежені чотирма годинами.
5. Password Management	7. Управління політикою корпоративних паролів і забезпечення її виконання
6. Session ID Management - Керування ідентифікаторами сеансів	8. Функція запуску та зупинки сеансу 9. Застосовує корпоративні політики доступу та контролю в кожному робочому сеансі, наприклад обмеження сеансів за допомогою Secure Shell (SSH) або протоколу віддаленого робочого столу (RDP) або обмеження дозволеного використання програм у цільовій системі
7. Сховище паролів	10. Забезпечує безпечне зберігання поточного пароля для кожного привілейованого облікового запису, керованого системою PAM
8. Emergency Access - Екстрений доступ	11. Використання PAM у непередбачених або надзвичайних ситуаціях, коли доступ до привілейованих облікових записів потрібен неочікуваним користувачам (привілейованим або непривілейованим)
9. Automated Account - Автоматизований обліковий запис	12. Автоматичний пошук підприємства для доказів і ідентифікації привілейованих облікових записів, таких як адміністратори домену або облікові записи, які прямо чи опосередковано (через успадкування привілеїв) мають повноваження на рівні привілейованого облікового запису

10. Session Monitoring - Моніторинг сесії	13. Механізм ідентифікації, реєстрації та попередження про аномальну діяльність привілейованого облікового запису
11. Session Replay - Повтор сеансу	14. Огляд сеансу для навчання та огляд подій і розслідувань
12. Моніторинг безпеки	15. Ведення журналів і аудит забезпечують зберігання журналів, аналіз і компоненти сповіщень
13. Лабораторне середовище	16. Віртуальні машини, мережі, маршрутизація, брандмауери тощо.

PAM — це домен у рамках керування ідентифікацією та доступом (IdAM), який зосереджується на моніторингу та контролі прав доступу, призначених привілейованим користувачам для їхніх привілейованих облікових записів. До привілейованих облікових записів належать локальні, доменні та системні адміністративні облікові записи, а також облікові записи програм, керування програмами та сервісні облікові записи. Ці облікові записи також можна використовувати для отримання доступу та проведення транзакцій, які використовують критично важливі для бізнесу/високоцінні програми, такі як розрахунок заробітної плати, соціальні мережі, хмарні служби і людські ресурси.

Архітектура та еталонний дизайн PAM визначають набір можливостей і їхніх зв’язків, які, об’єднавши, можна використовувати для керування та моніторингу використання привілейованих облікових записів привілейованими користувачами як для локальних, так і для хмарних реалізацій. У цьому розділі представлено високорівневу архітектуру та еталонний дизайн для реалізації такого рішення. Еталонний дизайн включає широкий набір можливостей, доступних на ринку, щоб проілюструвати повний спектр можливостей PAM, які може реалізувати організація. NCCoE розуміє, що організації можуть не знадобитися всі ці можливості. Організація може вибрати впровадження підмножини зображених можливостей, залежно від своїх рішень щодо управління ризиками.

Рішення PAM розроблено для вирішення функцій безпеки та підкатегорій, описаних у Таблиці 2.1 і складається з можливостей, зображених на Рис.2.6 та 2.7.

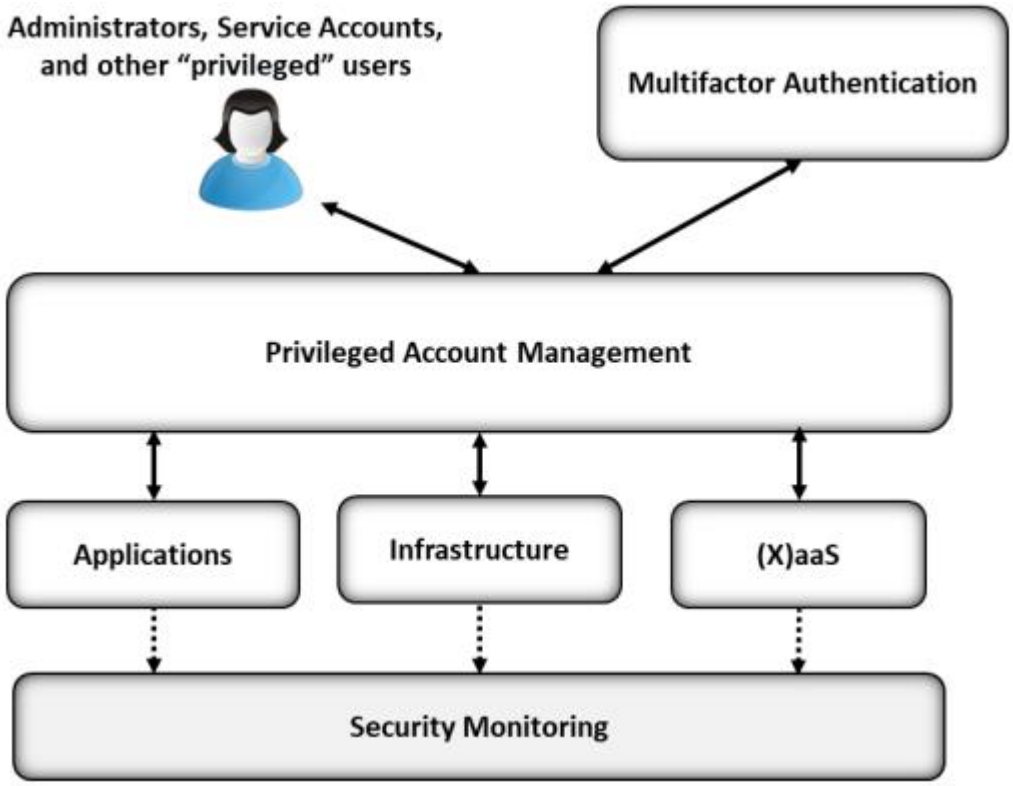

Рис.2.6. Архітектура високого рівня [4]

На рисунку 2.6 зображено архітектуру PAM у контексті організації. [4] Система PAM призначена для посередництва/контролю доступу та використання привілейованих облікових записів між корпоративними системами та службами та авторизованими «привілейованими» користувачами. На рис2.6 «(X)aaS» означає «[заповніть порожнє місце] як послугу DRAFT NIST SP 1800-18B: Privileged Account Management for the Financial Services Sector 27», наприклад програмне забезпечення як послуга (SaaS).), платформа як послуга (PaaS) і хмарні служби інфраструктури як послуги (IaaS). Нижче наведено приклади кожної з цих хмарних служб:

– SaaS: електронна пошта, програмне забезпечення для управління взаємовідносинами з клієнтами;

– PaaS: розробка додатків, потокові сервіси;

– IaaS: кешування, зберігання, мережа.

Еталонний дизайн, показаний на рис 2.7, зображує детальний дизайн PAM, включаючи зв'язки між можливостями, які складають дизайн . [4]

.

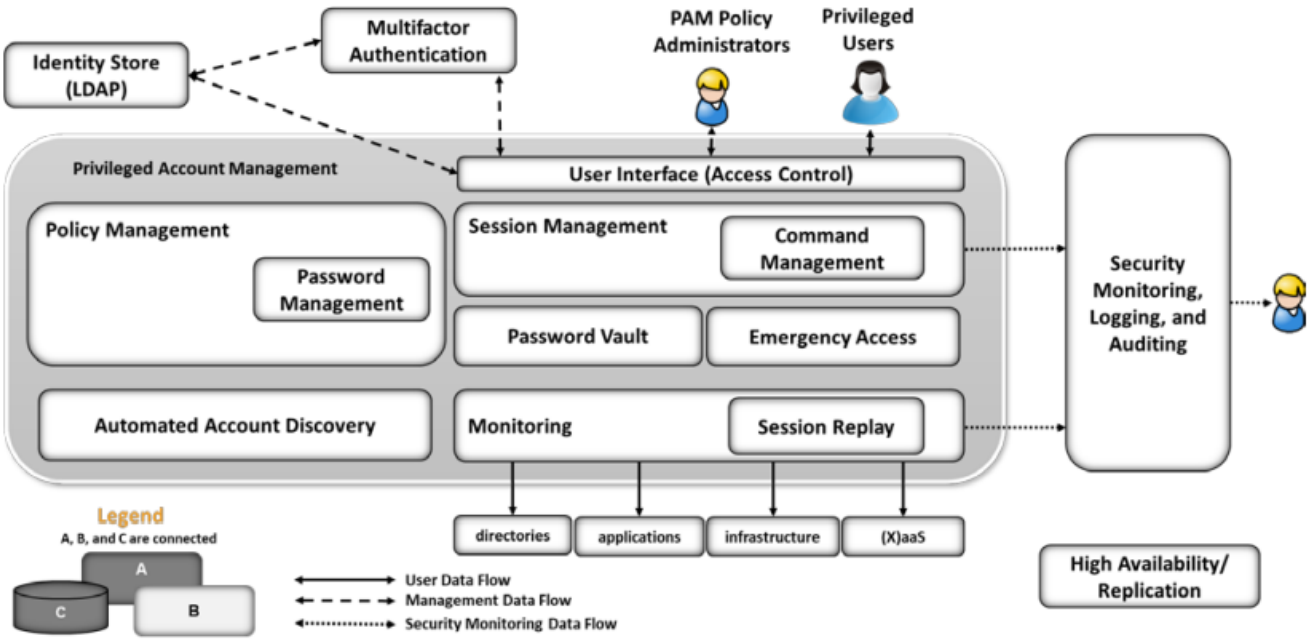

Рис.2.7. Еталонний дизайн PAM [4]

Суцільні лінії на Рис.2.7 представляють потік даних користувача між привілейованими користувачами та системами всередині підприємства. Пунктирні лінії представляють потік даних керування між компонентами архітектури PAM. Малі пунктирні лінії представляють потік даних моніторингу безпеки (журнали). Можливості/компоненти PAM коротко описані нижче:

1. Сховище ідентифікаційних даних (LDAP) надає репозиторій ідентифікаційних даних, спеціально зарезервований для привілейованих користувачів організації.

2. MFA дозволяє використовувати два або три фактори автентифікації для підвищення рівня автентифікації для привілейованих користувачів (див. NIST 800-63B [3] для більш детального опису вимог до факторів автентифікації).

3. Інтерфейс користувача забезпечує автентифікацію під час входу та інтерактивний інтерфейс користувача-PAM-системи, через який користувачі взаємодіють, щоб встановити або запитати робочі сеанси для кожної системи, якою вони адмініструють або до якої мають доступ для виконання своїх робочих функцій.

4. Управління політиками підтримує корпоративні політики доступу та контролю привілейованих користувачів, наприклад обмеження сеансів привілейованих користувачів до чотирьох годин.

5. Керування паролями підтримує та забезпечує дотримання корпоративних політик паролів.

6. Керування сеансами забезпечує дотримання корпоративних політик доступу та контролю в межах кожного робочого сеансу, наприклад обмеження сеансів SSH або RDP або обмеження дозволеного використання програм у цільовій системі.

7. Сховище паролів забезпечує безпечне зберігання поточного пароля для кожного привілейованого облікового запису, яким керує система PAM.

8. Екстрений доступ забезпечує використання PAM у непередбачуваних або надзвичайних ситуаціях, коли доступ до привілейованих облікових записів потрібен неочікуваним користувачам (привілейованим або непривілейованим).

9. Автоматизоване виявлення облікових записів шукає на підприємстві докази та ідентифікацію привілейованих облікових записів, таких як адміністратори домену або облікові записи, які прямо чи опосередковано (через успадкування привілеїв) мають повноваження на рівні привілейованого облікового запису.

10. Моніторинг сеансу забезпечує механізм для виявлення, реєстрації та попередження про аномальну активність, а також для навчання в режимі реального часу для використання привілейованого облікового запису.

11. Повтор сеансу забезпечує перегляд сеансу для навчання та огляд подій і розслідування.

12. Моніторинг безпеки, ведення журналів і аудит забезпечують зберігання журналів, аналіз і сповіщення компонентів, які зазвичай називаються інформацією про безпеку та керування подіями (SIEM).

13. UBA здійснює моніторинг діяльності привілейованих користувачів щодо діяльності або дій, які вважаються несподіваними або поза загальновизнаною моделлю діяльності.

14. Висока доступність/реплікація забезпечує доступність рішення PAM.

Системи PAM зазвичай використовують один із двох методів контролю доступу та використання облікового запису: розширення облікового запису або спільне використання облікового запису. Метод ескалації облікового запису збільшує привілейовану/авторизовану активність для особистого облікового запису кожного користувача протягом сеансу з цільовою системою на основі організаційних політик. Після завершення кожного сеансу обліковий запис користувача повертається до «нормального»/непривілейованого рівня авторизації. Техніка спільного використання облікових записів використовує набір привілейованих облікових записів, які спільно використовуються авторизованими привілейованими користувачами. Паролі для цих облікових записів зазвичай змінюються автоматично залежно від використання або часу. Наприклад, PAM-системи спільного використання облікових записів можуть бути налаштовані на зміну пароля для кожного облікового запису після кожного сеансу, під час якого він використовується, або, якщо він не використовується, через певний проміжок часу. Деякі організації можуть використовувати систему PAM для спільного використання облікових записів з унікальними обліковими записами PAM для окремих користувачів. Цей підхід може забезпечувати спрощений аналіз журналів для криміналістичних і навчальних цілей, оскільки цільова система записуватиме кожного унікального користувача у своїх журналах.

Перелічені вище компоненти працюють разом, щоб забезпечити функціональність PAM. Інтерфейс користувача використовує сховище

ідентифікаційних даних і MFA для автентифікації привілейованих користувачів і є інтерфейсом, через який користувачі взаємодіють із системою PAM. Користувачами PAM можуть бути люди або системи, наприклад програми. У системах PAM, які реалізують спільний доступ до привілейованого облікового запису, керування сеансами встановлює сеанси для кожного користувача до вибраної ними системи на основі політик у системі керування політиками. Керування сеансами також використовує сховище паролів для отримання паролів для цільових систем. Кожна сесія встановлюється за допомогою систем моніторингу та відтворення сесії відповідно до корпоративних політик моніторингу та запису сесії. Цільова система та система PAM реєструють діяльність кожного привілейованого користувача та надсилають журнали до SIEM для аналізу та попередження про аномальні події та умови. У системах PAM, які реалізують методи ескалації облікових записів для керування привілейованими користувачами, система керування сеансами підвищує привілеї кожного користувача на час сеансу з цільовою системою на основі політик у системі керування політиками. Керування сеансом відстежує сеанс, щоб повернути рівень привілеїв облікового запису до нормального стану після того, як користувач завершить сеанс. Управління сеансами також реєструє запити облікових записів користувачів і деталі запитів сеансів відповідно до політик підприємства. Цільові системи реєструють діяльність кожного привілейованого користувача та надсилають журнали до SIEM. NIST SP 800-92, Guide to Computer Security Log Management [5], було використано для впровадження та налаштування SIEM. SIEM зберігає журнали, створені кожною системою, і виконує аналітику для виявлення аномальної активності. Про аномальну активність повідомляється аналітикам безпеки. Автоматизоване виявлення облікових записів забезпечує підприємству постійний моніторинг облікових записів, які можуть вважатися привілейованими, і внесення змін до цих облікових записів. На основі політики підприємства адміністратори PAM можуть включити ці нещодавно визначені привілейовані облікові записи в систему PAM. Автоматичне виявлення облікових записів також можна використовувати для

сповіщення аналітиків безпеки про зміни облікових записів у привілейованих облікових записах або спробу ескалації непривілейованого облікового запису. Компоненти високої доступності/реплікації визначені в архітектурі, щоб підкреслити необхідність забезпечення високої доступності системи PAM. Підприємство може виявити, що підмножини компонентів достатньо для задоволення його потреб у зниженні ризику. UBA та компоненти високої доступності/реплікації не були включені до прикладів рішень, реалізованих у лабораторії NCCoE. Компонент високої доступності/реплікації не було включено через обмежений обсяг впровадження репрезентативної корпоративної інсталяції лабораторії NCCoE. Рішення UBA призначені для виявлення поведінки, що викликає занепокоєння, шляхом об'єднання всіх відповідних даних (наприклад, дії в мережі та на основі клієнта/хоста, системи людських ресурсів, звіти співробітників, публічні записи, записи про подорожі), а потім для пошуку значущих моделей поведінки. Наприклад, рішення UBA може виявити, що була запущена атака, наприклад атака на підвищення привілеїв (в ідеалі на ранніх стадіях формування цієї атаки). UBA не було включено до прикладів реалізації через відсутність відповідних даних, необхідних для ефективного аналізу моделі поведінки. Оскільки методи UBA дуже різноманітні, UBA для PAM можуть бути розглянуті організаціями, які можуть визначити конкретні аспекти поведінки та аналізу, важливі для їх середовища та рішень щодо управління ризиками.

3 РОЗРОБКА ВАРІАНТУ ТЕХНОЛОГІЇ ПРИВІЛЕЙОВАНОГО ДОСТУПУ PRIVILEGE MANAGER РІШЕННЯ DELINEA

3.1. Privilege Manager рішення Delinea для керування привілеями кінцевих точок і керування додатками для робочих станцій

Privilege Manager Delinea надає такі можливості [6]:

Розгорнути та використати одного агента - знаходить програми з правами адміністратора навіть на комп'ютерах, які не належать до домену, і застосовуйте політики.

Визначити гнучку політику – підвищити, дозволити, заборонити та обмежити програми лише кількома клацаннями за допомогою майстра політики.

Управління/вилучення прав локального адміністратора - створювати правила для постійного визначення членства в локальній групі та автоматичної ротації привілейованих облікових даних нелюдей.

Підвищити права програми - дозволяє довіреним програмам запускати, блокувати інші або використовувати їх у ізольованому середовищі, зберігаючи модель найменших привілеїв.

Підвищення продуктивності IT і кінцевих користувачів - заявки служби підтримки зменшуються завдяки автоматизованим масовим або повторюваним операціям; люди автоматично отримують доступ до потрібних програм і систем.

Розробимо згідно вимог [4] до архітектури PAM схеми еталонної архітектури Privilege Manager Delinea.

Основні компоненти Privilege Manager Delinea [6] :

Користувач програми – це користувачі, які підключаються до веб-сайтів Privilege Manager. Ці користувачі обмежуватимуться користувачами, які виконують адміністративні завдання (адміністратори), використовуватимуть рішення в ролі служби підтримки або виконують затвердження чи аудит.

Агенти керування привілеями – використовуються для контролю програм і керування локальними користувачами/групами.

Балансувальники навантаження – балансувальники навантаження часто задіяні в рішенні, щоб допомогти розподілити веб-трафік між більш ніж одним веб-сервером. Локальні та глобальні балансувальники навантаження, якщо вони доступні, можуть використовуватися в рішенні для подальшого скорочення потенційного простою додатків під час оновлення, виправлення та збоїв на одному сайті.

Веб-сервер - це основний компонент рішення. Наші веб-сервери використовують IIS 7 і новіші версії та працюватимуть лише на Windows Server 2008 R2 – Windows Server 2016. Для кількох веб-серверних (кластерних) рішень саму веб-програму можна зробити кластерною. Кожен веб-сервер діє як окремий окремий веб-сервер.

Сервер бази даних – це основний компонент рішення. Microsoft SQL Server розміщує бази даних Privilege Manager. Вони сумісні лише з SQL Server 2012 або новішою версією, що працює на Windows Server 2012 R2 - Windows Server 2016. Бази даних Thycotic можна розмістити на окремому сервері, FCI або бажано використовувати AlwaysOn AG для кластерних середовищ. Бази даних можна додати до існуючого робочого кластера або екземпляра SQL, але потрібно правильно визначити розмір середовища. Рекомендується лише автентифікація Windows.

Зворотнє проксі/службова шина Azure. Правильно налаштований зворотний проксі діятиме як буфер між агентами Privilege Manager і сервером(ами) Privilege Manager, щоб обмежити доступ до сервера. Можна використовувати шину Azure, щоб запобігти підключенню кінцевих точок агента безпосередньо до вашого веб-сервера Privilege Manager.

Секретний сервер. Додатково можна інсталювати секретний сервер із Privilege Manager, щоб використовувати джерело автентифікації та сховище для облікових даних Privilege Manager. Використання секретного сервера як джерела автентифікації для Privilege Manager дозволяє використовувати параметри MFA для входу. Крім того, призначення ролі програми можна призначити в Secret Server. Якщо використовуються функції секретного сервера (крім автентифікації та сховища для диспетчера привілеїв), секретний сервер має бути на окремих серверах.

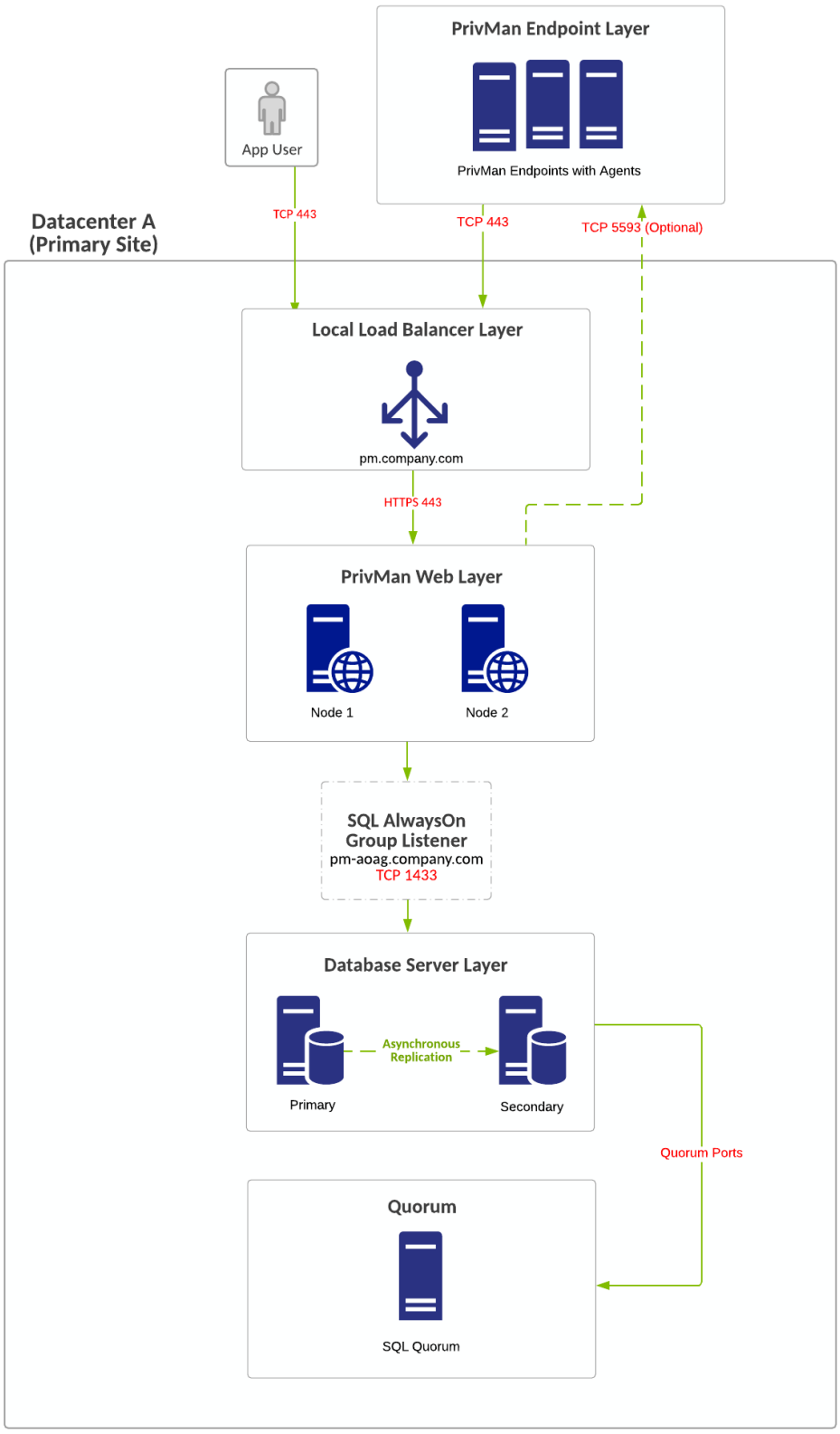

Рис. 3. 1 Схема Privilege Manager

Агенти диспетчера привілейованого доступу

Агенти диспетчера привілеїв є важливим компонентом контролю додатків та локальної безпеки Delinea, надаючи можливість оцінювати працездатність та статус кінцевих точок у режимі реального часу. Агенти необхідні на кінцевих комп'ютерах для реалізації політик Privilege Manager [7].

Privilege Manager надає звіти про стан агентів і операційних систем кінцевих точок, що попередньо налаштовані і повністю настроюються. На панелі звітів Privilege Manager можна деталізувати звіти за будь-яким параметром і легко експортувати дані звіту до інших програм для створення звітів або Excel.

Privilege Manager підтримує агенти на:

– Windows
– macOS
– Unix/Linux

Щоб локальні адміністратори не втручалися в роботу агентів Delinea, які працюють у їх системі, адміністратори диспетчера привілеїв можуть призначати користувачів, які можуть запускати та зупиняти служби диспетчера привілеїв, що працюють на кінцевих точках, такі як агент Delinea або керування програмами Delinea.

Розглянемо приклад редагування політики обмеження дозволів облікового запису в службах агента (Windows) [7,8].

Користувач або група має бути доступна в диспетчері привілеїв, щоб бути обраною під час налаштування завдання. Цей користувач або група матиме права запускати та зупиняти служби агентів, що працюють на кінцевих точках, після ввімкнення політики обмеження дозволів облікового запису на служби агентів (Windows). [7,8].

Редагування У групі комп’ютерів виберіть «заплановані завдання» .

– Знайдіть Обмежити обліковий запис.

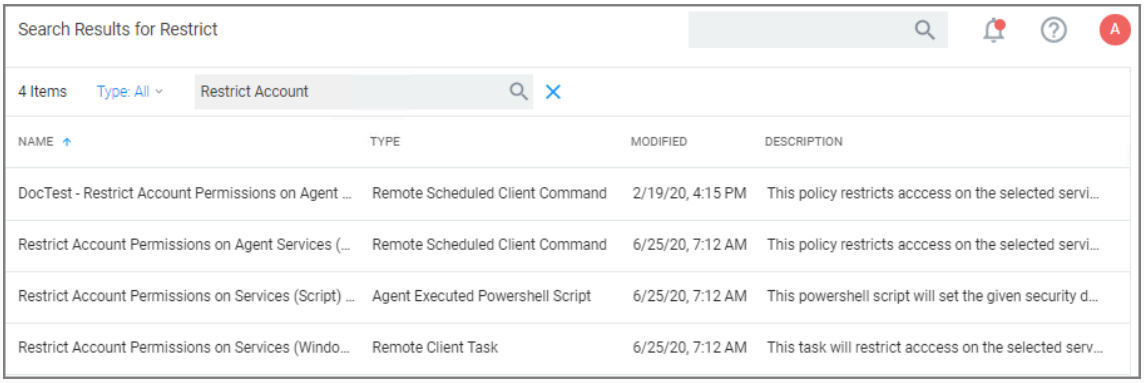

Рис. 3.1. Обліковий запис

1. Натисніть політику «Обмежити дозволи облікового запису в службах агента» (Windows) (Рис. 3.2).

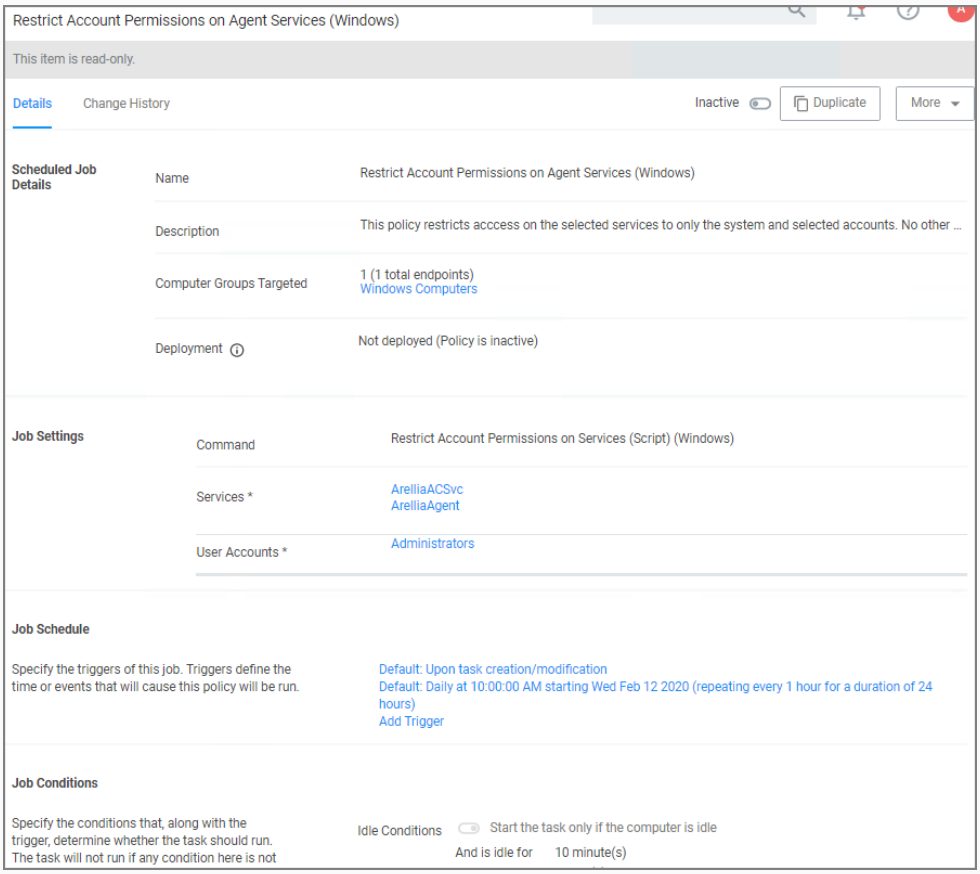

Рис. 3.2. Налаштування політик

2. Щоб налаштувати політику, натисніть **Дублювати** [7,8].

3. Налаштуйте назву скопійованої політики та натисніть « **Створити** » (Рис. 3.2.) [7,8].

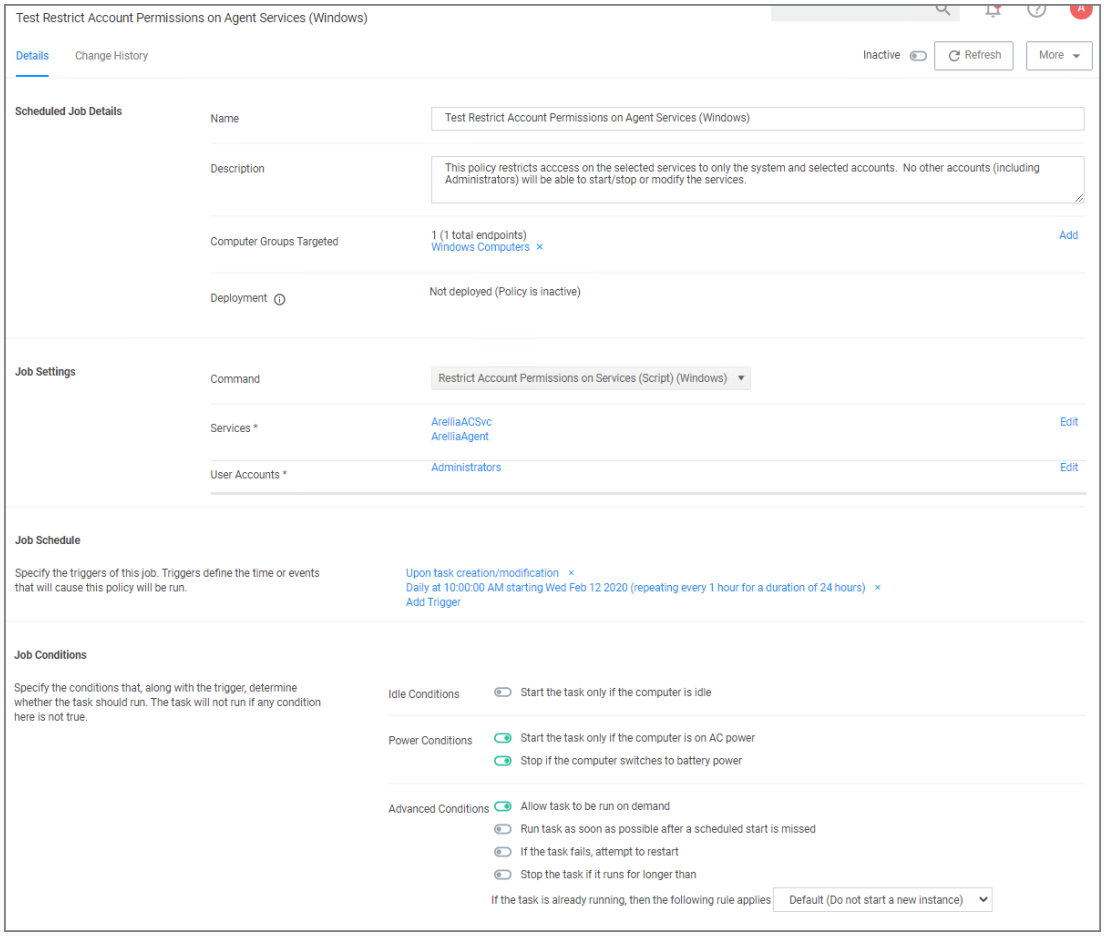

Рис. 3.3. Створення політики

4. Налаштуйте політику
   - Деталі запланованої роботи.
   - Налаштування роботи.
   - Графік роботи.
   - Умови роботи.

5. У розділі « **Служби** » за замовчуванням присутні служба керування програмами Arellia та служба агентів Arellia. Додайте будь-які служби, які ви також можете захистити. Використовуйте поле пошуку, щоб знайти та вказати інші назви послуг.

6. Для **облікових записів користувачів** скористайтеся **Редагувати** та скористайтеся полем пошуку, щоб знайти певні облікові записи користувачів, які мають дозволи вносити зміни до вказаних служб. Адміністратори присутні за

замовчуванням, якщо ви хочете обмежити лише підмножину користувачів із правами адміністратора, створіть групу та оновіть відповідним чином.

7. Натисніть **Зберегти зміни**.

8. Установіть для політики значення **Active**.

Кінцеві точки macOS

В даний час неможливо заборонити обліковий запис локального адміністратора в macOS запускати та зупиняти фонові служби, такі як агент Privilege Manager.

Встановлення поштового агента

Коли ваші агенти встановлені, ви можете перевірити стан працездатності ваших агентів з точки зору стану реєстрації та стану політики на домашній сторінці. Для цього необхідно перейти до Admin | Агенти для отримання додаткової інформації про встановлених агентів.

Іконки "Стан агента" показують, скільки у вас керованих операційних систем, а також стан реєстрації вашого агента (агентів) та стан політики. Якщо ви натиснете на шкалу стану реєстрації агента, ви побачите звіт зі списком машин (стовпець «Моніторинг ресурс»), на яких встановлений кожен зареєстрований агент.

Клацнувши диск «Стан політики агента» на домашній панелі, ви потрапите у звіт, який пов'язує всі ваші машини, зареєстровані агентом, з кількістю відсутніх політик для кожного агента. Ця сторінка стане безцінною, коли у вас буде кілька політик, які працюють на різних групах комп'ютерів у вашій мережі.

Після встановлення агентів необхідно переконатися, що вони зареєстровані у Privilege Manager. Перейдіть до будь-якого (Рис. 3.4):

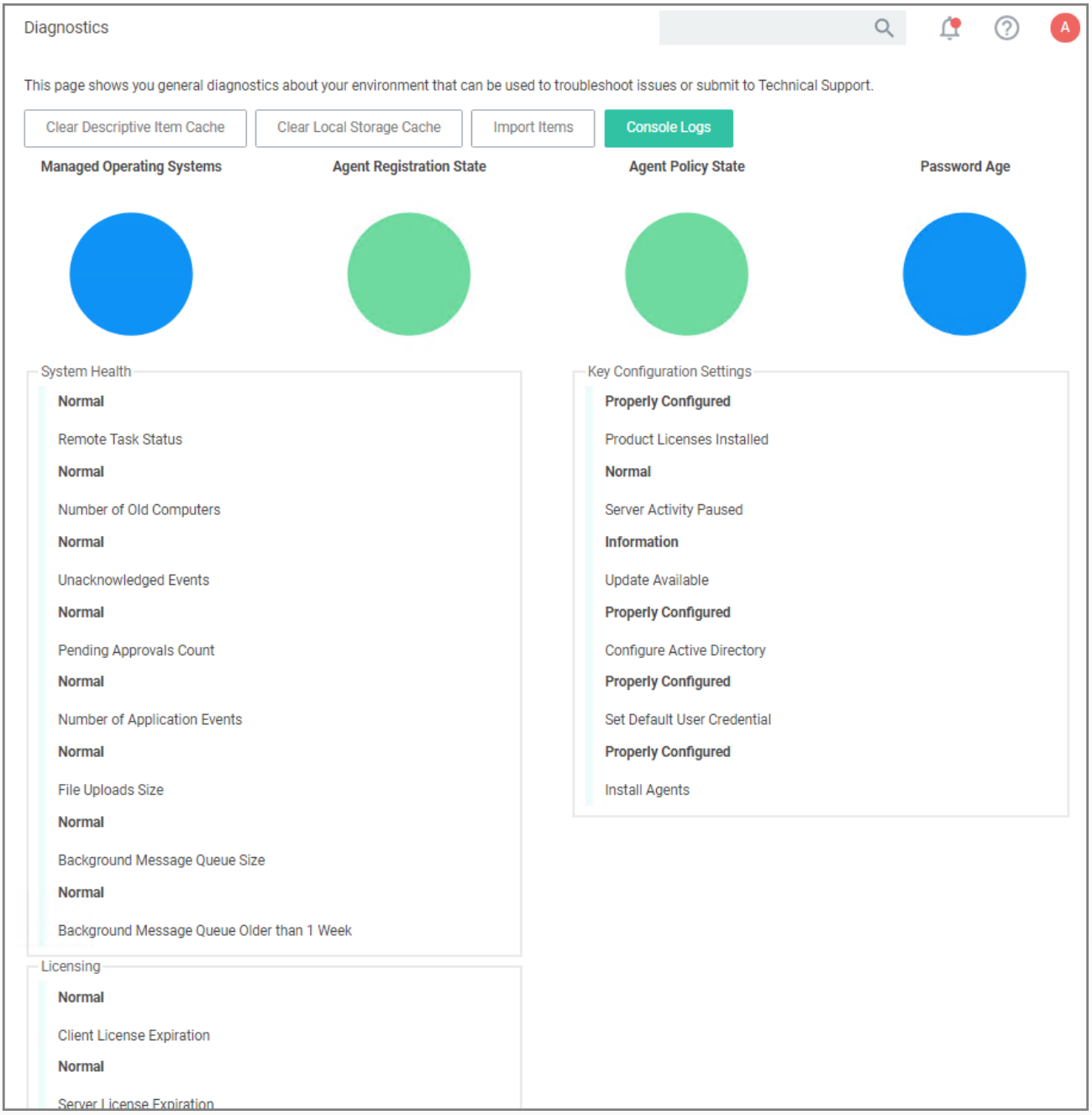

Рис. 3.4. Панель агенти Privilege Manager

Дії АДМІНІСТРАТОР | Агенти, щоб переглянути дані свого агента [9] (Рис. 3.5).

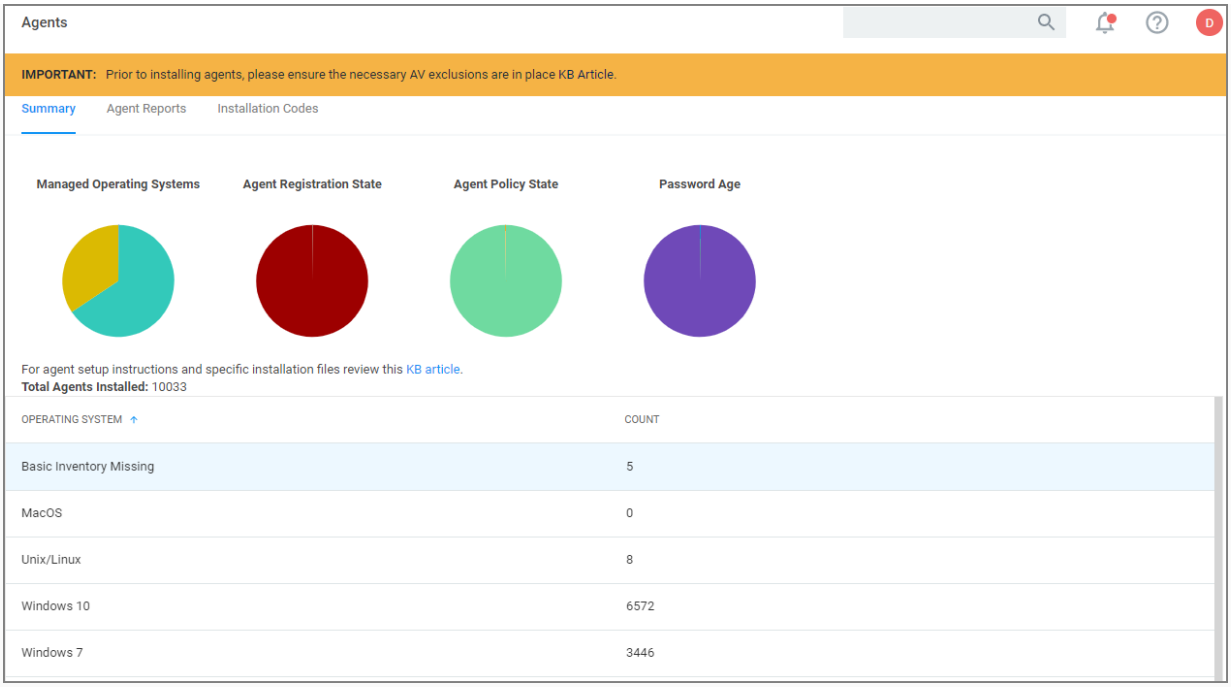

Рис.3.5. Перегляд даних агенту

Після отримання початкових політик майбутні оновлення базуватимуться на розкладах завдань, установлених у політиках Оновлення відповідних політик і політиках запланованої реєстрації. Переконайтеся, що вибрано правильні політики на основі операційних систем Windows або Mac. Щоб змінити ці розклади, необхідно перейти до необхідної групи комп'ютерів і виберати «*Заплановані завдання*». Тригери можна налаштувати в розділі «Розклад завдань» [8].

На сторінці відомостей про агента є можливість побачите кількість зареєстрованих агентів і операційну систему, запущену на зареєстрованих кінцевих точках. Зареєстровані кінцеві точки також можна переглянути у звіті *Agent Installation Summary*, перейшовши на вкладку *Agent Reports* [8].

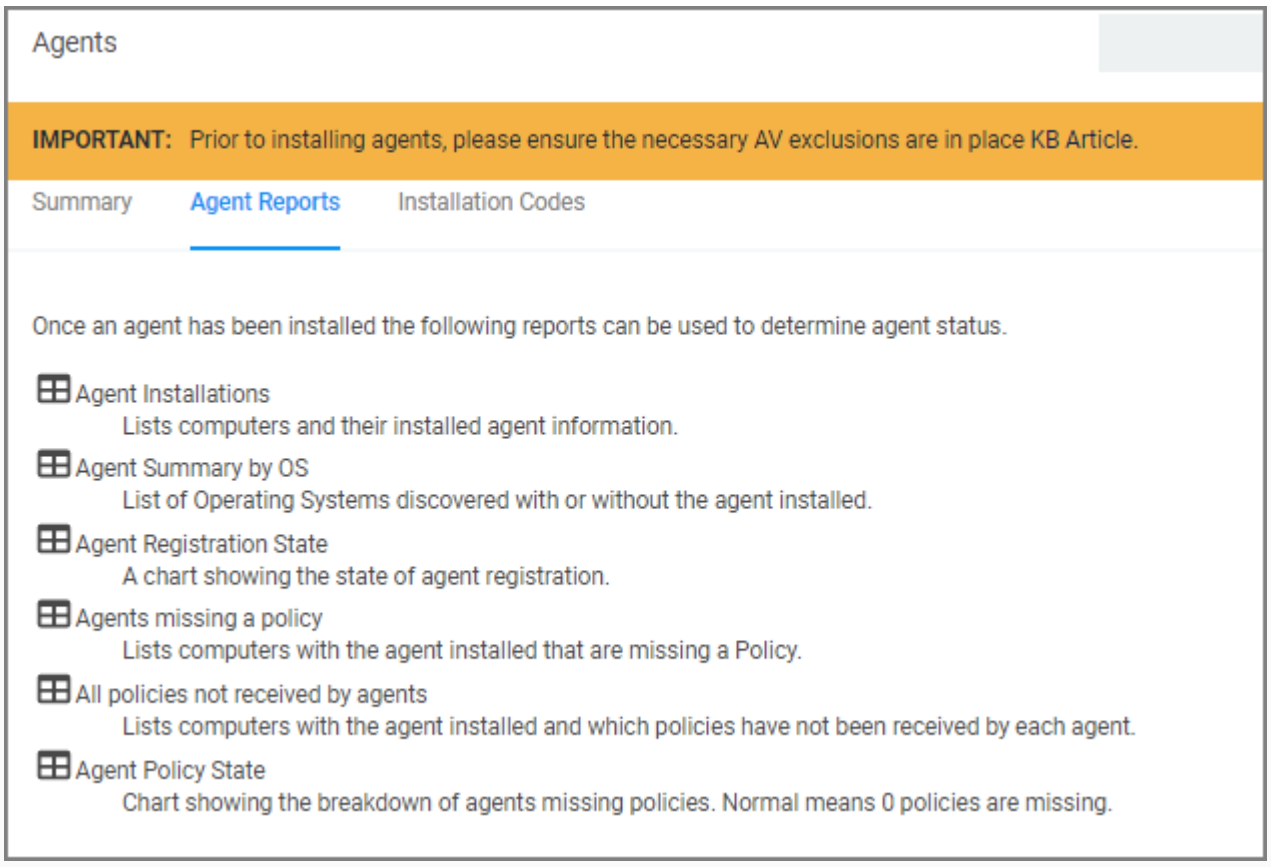

Рис.3.6. Відомості про агента [8]

Шифрування агента

Трафік агента захищено через SSL/TLS (1.2).

Специфічні завдання агента

Певні завдання Privilege Manager безпосередньо пов'язані з процесами агента та їх робочими навантаженнями.

Завдання на стороні сервера, також відомі як заплановані команди віддаленого клієнта, не потребують політики. Завдання агента потребують політики. Ці типи завдань, за винятком одного, увімкнено за замовчуванням і виконуються за розкладом. Більшість є системними завданнями лише для читання, які можна копіювати, перейменовувати та потім налаштовувати.

Більшість запуститься вперше після ініціалізації системи.

Заплановані команди віддаленого клієнта Windows [7,8].

Таблиця 3.1

Заплановані команди віддаленого клієнта Windows

Ім'я	Опис	Розклад	Увімкнено
Обмеження дозволів облікового запису в службах агента (Windows)	Наказує комп’ютерам дозволяти лише вказаним користувачам запускати та зупиняти служби Delinea.	n/a	Ні
Основний інвентар (початковий, Windows)	Вказує комп’ютерам повідомляти серверу WMI-класи Win32_ComputerSystem, Win32_ComputerSystemProduct і Win32_OperatingSystem.	щодня	Так
Основний інвентар (Windows)	Вказує комп’ютерам повідомляти серверу WMI-класи Win32_ComputerSystem, Win32_ComputerSystemProduct і Win32_OperatingSystem.	щодня	Так
Перенесення інвентаризації агента очищення (Windows)	Завершує та очищає передачі BITS і тимчасові файли, які використовує TMS Agent Inventory Helper.	щодня	Так
Очищення, надіслані події диспетчера привілеїв (Windows)	Очищає події агента, які були успішно передані з керованих кінцевих точок, щоб звільнити дисковий простір.	щодня	Так
Налаштувати диспетчер привілеїв, видалити програми	Налаштуйте поведінку видалення програм диспетчера привілеїв.	щодня	Так

Ім'я	Опис	Розклад	Увімкнено
Політика інвентаризації файлів за замовчуванням (Windows)	Метою цієї політики є інвентаризація програмного забезпечення, запущеного на керованому комп’ютері.	щотижня	Так
Розгорнути налаштування виключення хешу файлу (Windows)	Метою цієї політики є надання можливості виключати певні розширення файлів із процесу хешування.	щодня	Ні
Переконайтеся, що параметр заміни UAC (Windows)	Переконайтеся, що встановлено ключ реєстру UAC Override.	щодня	Так
Політика локального інвентаризації користувачів	Метою цієї політики є інвентаризація облікового запису локального користувача, груп і членства в групах на клієнті. Цю політику також можна використовувати для інвентаризації певних привілеїв облікового запису.	щотижня	Так
Виконайте пошук ресурсів (Windows)	Розклад, за яким агенти перевірятимуть сервер, щоб визначити, чи потребують виявлення будь-які локальні ресурси.	щодня	Так
Повторити помилкові події TMS (Windows)	Сканувати чергу агента для будь-яких подій, які потребують повторної передачі.	щодня	Так
Запланована перевірка незавершених завдань клієнта – Інтернет-клієнти (Windows)	Ініціювати перевірку завдань клієнта, що очікують на виконання. Використовується агентами, які не можуть отримати вхідне з’єднання від сервера.	щодня	Так

Ім'я	Опис	Розклад	Увімкнено
Реєстрація за розкладом - Інтернет-клієнти (Windows)	Ініціювати реєстрацію агента на сервері рідше, ніж на внутрішніх клієнтах.	щодня	Так
Реєстрація за розкладом (Windows)	Ініціювати реєстрацію агента на сервері.	щодня	Так
Команди агента оновлення (Windows)	Наказує агенту оновити будь-які команди агента, якщо потрібно.	щодня	Так
Оновлення застосовних політик – Інтернет-клієнти (Windows)	Наказує агенту перевірити на сервері наявність змін у політиці.	щодня	Так
Оновлення застосовних політик (Windows)	Наказує агенту перевірити на сервері наявність змін у політиці.	щодня	Так
Оновити надані клієнтські елементи ресурсів (Windows)		щодня	Так
Політика інвентаризації входу користувача	Оновлює дані для входу користувача за вказаним розкладом.	щотижня	Так
Політика інвентаризації служби Windows	Метою цієї політики є інвентаризація служб Windows на клієнті.	щотижня	Так

Розгортання гібридної мультитенантної хмарної архітектури Secret Server

Гібридна мультитенантна хмарна архітектура Secret Server (SSC) Ця стандартна архітектура SSC є «гібридною мультитенантною», тому що лише інтерфейс є мультитенантним — він спільний з іншими клієнтами . Бази даних, службові шини та облікові записи зберігання є єдиними клієнтами (рис 3.4). [9]

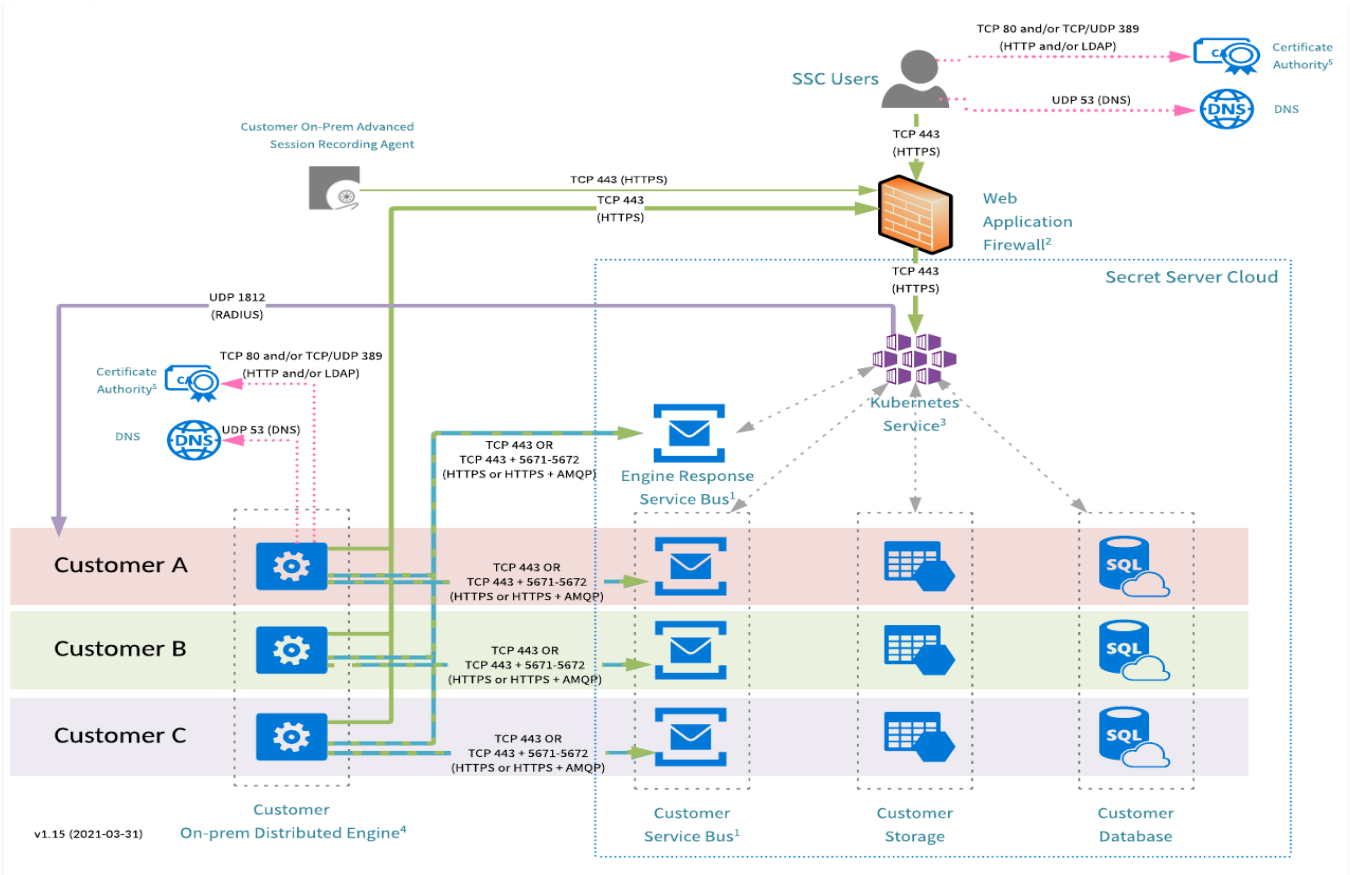

Рис.3.7. Хмарна архітектура секретного сервера [9]

На рис.3.7. Стрілки вказують напрямок початкового підключення.

1: Службові шини

Додавання IP-адрес до дозволеного списку не є обов'язковим, якщо не діють правила вихідного брандмауера. Якщо необхідний білий список IP-адрес, необхідно зв'язатися зі службою підтримки Delinea, щоб отримати спільну службову шину відповідей движка та імен хостів спеціальної шини обслуговування клієнтів. Вимога до TCP-порту залежить від типу транспорту, налаштованого в налаштуваннях розподіленого механізму. За замовчуванням використовуються веб-сокети, для яких потрібен TCP 443. Якщо в програмі вибрано параметр AMQP, також потрібні порти TCP 5671/5672. [9]

2: Брандмауер веб-додатків (WAF)

Додавання IP-адрес до дозволеного списку не є обов'язковим, якщо не діють правила вихідного брандмауера. Як правило, загальнодоступна IP-адреса, яку визначає ім'я хосту, залежить від географічного розташування джерела запиту. Щоб забезпечити безперебійне з'єднання, усі наведені нижче IP-адреси мають бути в білому списку. [9]

Всі регіони:

- 45.60.32.37
- 45.60.34.37
- 45.60.36.37
- 45.60.38.37
- 45.60.40.37
- 45.60.104.37

3: RADIUS

Якщо налаштовано автентифікацію RADIUS, необхідний білий список вхідних повідомлень. IP адреси:

- secretservercloud.com:
  - 52.224.253.7 (основний)
  - 52.224.253.4 (основний)
  - 52.151.206.73 (основний)
  - 52.151.206.77 (основний)
  - 52.151.206.35 (основний)
  - 52.160.67.39 (DR)
  - 52.160.67.38 (DR)
  - 104.40.25.170 (DR)
  - 138.91.163.99 (DR)
  - 137.135.51.234 (DR)
- secretservercloud.ca:
  - 52.228.117.246 (основний)

    - 52.228.113.119 (основний)
    - 52.139.7.40 (основний)
    - 52.139.7.137 (основний)
    - 52.139.7.197 (основний)
    - 52.229.119.193 (DR)
    - 52.229.119.89 (DR)
    - 52.235.39.79 (DR)
    - 52.235.39.125 (DR)
    - 52.235.39.5 (DR)
- secretservercloud.eu:
    - 20.79.64.213 (Первинний)
    - 20.79.65.3 (основний)
    - 20.79.226.78 (Первинний)
    - 20.79.226.180 (основний)
    - 20.79.226.116 (основний)
    - 20.50.180.242 (DR)
    - 20.50.180.187 (DR)
    - 20.50.154.28 (DR)
    - 20.50.176.86 (DR)
    - 20.50.156.219 (DR)
- secretservercloud.com.sg
    - 20.195.97.220 (Первинний)
    - 20.195.98.154 (основний)
    - 20.212.128.73 (основний)
    - 20.212.128.75 (Первинний)
    - 20.212.128.74 (основний)
    - 65.52.165.108 (DR)
    - 65.52.160.251 (DR)

- 52.184.100.188 (DR)
- 52.184.101.189 (DR)
- 52.184.101.213 (DR)

- secretservercloud.com.au:
  - 20.37.251.37 (Первинний)
  - 20.37.251.120 (основний)
  - 20.37.5.233 (Первинний)
  - 20.37.5.227 (Первинний)
  - 20.37.5.48 (Первинний)
  - 20.53.142.34 (DR)
  - 20.53.142.37 (DR)
  - 20.53.80.77 (DR)
  - 20.53.81.216 (DR)
  - 20.53.82.77 (DR)

4: Розподілений механізм (DE - Distributed Engine)

Якщо зовнішні клієнти повинні мати можливість підключатися до внутрішніх кінцевих точок SSH або RDP, проксі-сервер SSH можна налаштувати на DE. Крім того, TCP-порт 22 має бути відкритим для вхідних з'єднань на сервері DE, а також мати відповідну конфігурацію, щоб дозволяти вхідні з'єднання з загальнодоступного Інтернету.

5: CRL сертифікатів

Білий список не є обов'язковим, якщо не діють правила вихідного брандмауера. Якщо необхідно, може знадобитися доступ до CRL або кінцевих точок OSCP. Кінцеві точки CRL і OSCP можуть відрізнятися від клієнта до клієнта. Щоб визначити кінцеві точки, перегляньте сертифікати, надані:

- Брандмауер веб-додатків
- Шиною обслуговування клієнтів
- Сервісна шина реакції движка

- CDN для оновлень DE.

Інформаційна панель серверу секретів

Для управління сервером адміністратором безпеки використовується зручна інформаційна панель серверу секретів. Інформаційна панель серверу секретів складається з наступних компонентів.

- Активні сеанси моніторингу: ваш (рис.3.8) і поточні сеанси моніторингу.
- Схвалення: ваші поточні схвалення в процесі.
- Статус движка : прокручуваний список статусів підключення та активації розподіленого механізму.
- Heartbeat Status: графічне зображення поточного стану ваших Heartbeat Status: успіх, очікування або невдача. Якщо ви клацнете один із статусів, ви перейдете на сторінку звіту про цей статус. Наприклад, Reports > Secrets Failing Heartbeat . Якщо клацнути посилання « Поточний », ви перейдете на сторінку « Звіти» > «Стан за днями».
- Найчастіше використовувані секрети: таблиця секретів, до яких зверталися останнім часом, упорядкованих за датою та папкою.
- Ротація паролів: стан вашої поточної ротації паролів. Якщо ви клацнете посилання « Сьогодні » , ви перейдете на сторінку « Звіти» > «RPC за днями» .

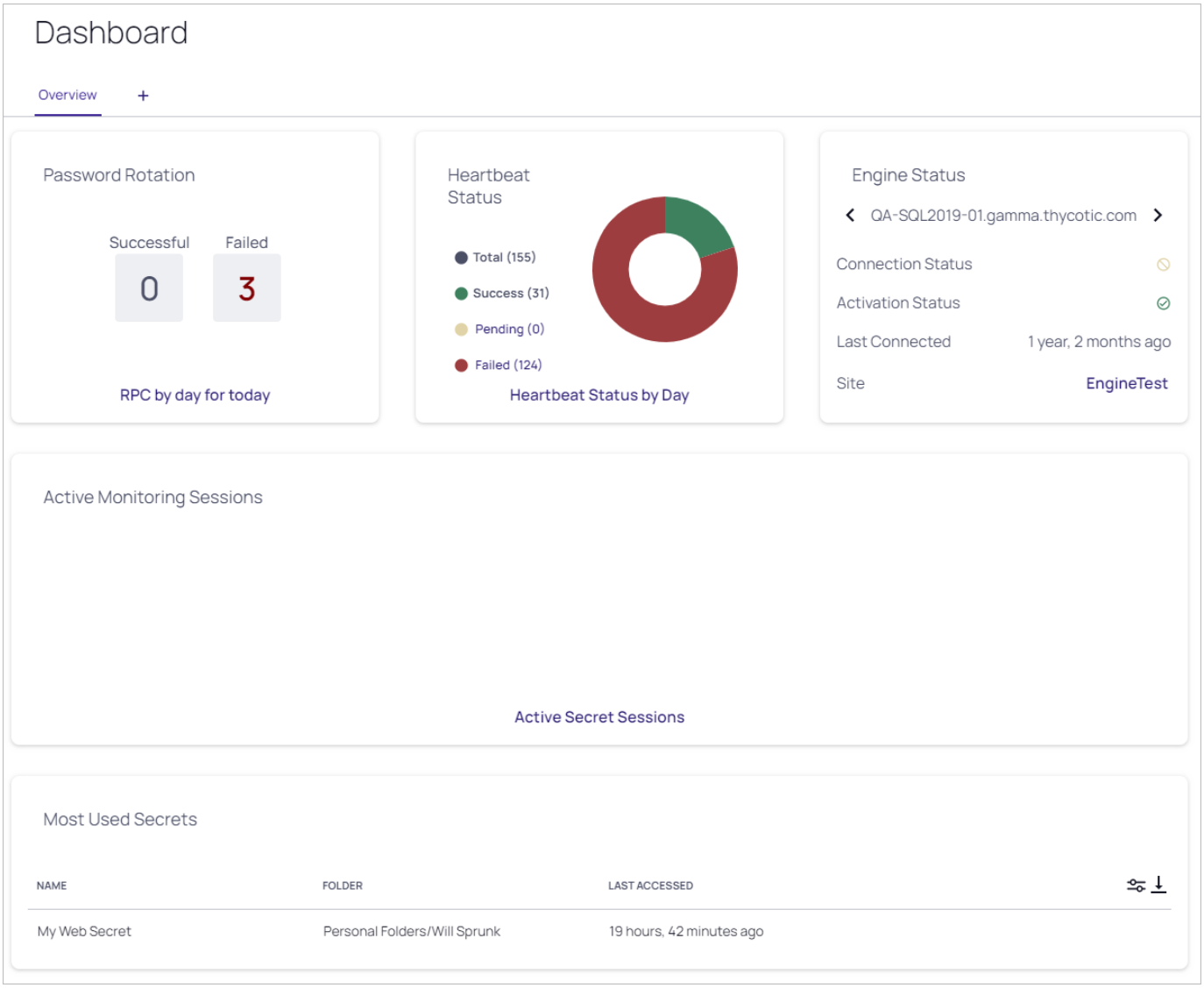

Рис. 3.8 Інформаційна панель сервера секретів [10]

Таким чином успішне налаштування всіх компонентів технології привілейованого доступу дозволить адміністраторам безпеки управляти доступом до інформаційної системи організації.

3.2. Розробка рекомендацій управління доступом привілейованого доступу

Захист критично важливих бізнес-додатків, хмарних ресурсів і віддалених співробітників на підприємстві без периметра за допомогою звичайних інструментів керування привілейованим доступом більше не прийнятний. Для боротьби з

сучасними кіберзагрозами, що розвиваються, командам IT-безпеки потрібні передові рішення привілейованого доступу, щоб отримати контроль над веб-платформами хмарного керування та забезпечити мінімальний доступ.

Розуміння того, як привілеї порушуються.

Узгодити привілейований доступ із вашими пріоритетами безпеки

Обирати «обов'язкові елементи» для рішення безпечного привілейованого доступу .

Практично у всіх організаціях є якісь невідомі або некеровані привілейовані облікові записи, що збільшує ризик компромісу. Це може статися з різних причин:

Для співробітників, які пішли, доступ ніколи не закривається організація.

Обліковий запис використовується рідко і стає застарілим або покинутим.

Облікові записи за умовчанням для нових пристроїв ніколи не вимикаються, а паролі залишаються незмінними.

Оскільки забезпечення продуктивності та безпеки працівників у середовищі для роботи з будь-якого місця вимагає значно іншого підхіду, дуже важливо мати розширене делегування та керування привілеями серед можливостей PAM.

Слід використовувати:

Контроль доступу на основі ролей (RBAC) дозволить налаштувати базовий рівень і доступ за замовчуванням для кожного віддаленого працівника для внутрішніх і веб-додатків. ти

Визначати та контролювати дії користувачів. встановити надійне сховище паролів. Для додаткового нагляду дуже важливо відстежувати, коли адміністратори перевіряють облікові дані та встановлювати часові обмеження для тимчасового доступу, якщо це необхідно. Моніторити елементи керування сеансом, такі як затвердження робочого процесу, подвійний контроль, реєстрація натискань клавіш і запис сеансу, додають додатковий рівень контролю.

Використання автоматизованих засобів запуску керування підключенням надає доступ до захищених ресурсів, не відкриваючи користувачеві пароль за допомогою введених облікових даних. Цей підхід допомагає перемістити паролі у фоновий режим, зменшуючи втому співробітників від паролів, а також суттєво зменшить ризики безпеки того, що хтось продасть або передасть пароль. Керування підключеннями є життєво важливим для аудиту, оскільки вони повідомляють зі 100% упевненістю, «хто був за клавіатурою» у конкретний час, коли використовувався спільний обліковий запис.

Уніфікований профіль. Віддалені співробітники та сторонні особи можуть використовувати власні робочі станції, включаючи ноутбуки та мобільні пристрої, у різних ситуаціях. Ви можете уніфікований профіль для кожного співробітника в усіх операційних системах і середовищах, як на місці, так і в хмарі. Таким чином ви дізнаєтесь, хто вони, коли вони отримують доступ до привілейованих облікових записів, незалежно від пристрою, який вони використовують.

Генерація складних паролів. Завдяки сучасним PAM-рішенням корпоративного рівня користувачам не потрібно запам’ятовувати паролі. Насправді їм зовсім не потрібно їх бачити. Високоякісне рішення PAM генерує складні паролі, автоматично змінює їх і використовує проксі-сервери для з’єднання систем, виключаючи людський елемент із рівняння.

Використовуйте моніторинг сесії. Спрощує для IT-команд налаштовувати та захищати будь-які сеанси.

Використовуйте автоматизацію PAM – це покращує видимість, контроль і нагляд Ефективні рішення PAM використовують багато можливості автоматизації для блокування доступу до привілейованого облікового запису та запобігання кібератакам.

Використовуйте примусова перевірку та ротація паролів. Інструменти PAM запобігають крадіжці облікових даних, забезпечуючи складні паролі та періодично змінюючи їх без переривання обслуговування.

Політики контролю програм. Інструменти PAM можуть блокувати зловмисне програмне забезпечення, застосовуючи правила на основі політики, які запобігають запуску відомих загроз або невідомих програм.

Використовуйте неперервне відкриття. Інструменти PAM можуть ідентифікувати привілейовані облікові записи та облікові дані та надавати детальну інформацію про їхній статус. Наприклад, вони можуть запитувати всі кінцеві точки щодо сертифікатів SSL, термін дії яких закінчується.

Використовуйте затвердження робочого процесу. Інструменти PAM можуть установлювати правила для розподілу обов’язків і послідовність кроків моніторингу та затвердження для забезпечення підзвітності та нагляду.

ВИСНОВКИ

В результаті виконання магістерської роботи було отримано наступні наукові результати:

Визначено мету, завдання та цілі управління привілейованим доступом на основі якого визначено необхідність створення привілейованих облікових записів, які надають можливість встановлювати або видаляти програмне забезпечення, оновлювати операційну систему або змінювати конфігурації системи чи програми.

В результаті аналізу визначено проблему щодо неправомірних дій, які можуть призвести до тримання привілеїв, в залежності від рівня доступу,який надається привілейованим обліковим записам.

В результаті аналізу існуючих технологій за магічним квадрантом Gartner було обрано Privilege Manager рішення Delinea, яке досягло прогресу у своїх можливостях керування секретами, а також отримала високі оцінки в управлінні життєвим циклом облікових записів служб.

Проведено дослідження моделі та методи контролю доступу.

Згідно міжнародних стандартів визначено архітектуру та визначено життєвий цикл управління привілейованим доступом в якому визначено до стратегії найменших привілеїв щодо визначання, постійного пошуку, контролю, аудиту, моніторингу та дослідження поведінки привілеїв.

В результаті роботи отримано варіант схеми технології Privilege Manager рішення Delinea та надано рекомендації щодо управління привілейованим доступом фахівцям з кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. PAM доступ [Електронний ресурс] – Режим доступу: https://www.ssh.com/academy/iam/privileged-account .
2. Управління привілейованими обліковими записами [Електронний ресурс] – Режим доступу: https://medium.com/@JeffDF/the-security-sector-to-watch-privileged-account-management-442faf57b03e
3. Ппп
4. https://www.gartner.com/doc/reprints?id=1-2AMLFOI1&ct=220720&st=sb
5. PAM-NIST-SP1800-18b [Електронний ресурс] – Режим доступу: https://www.nccoe.nist.gov/sites/default/files/legacy-files/fs-pam-nist-sp1800-18b-draft.pdf
6. Привілейований доступ [Електронний ресурс] – Режим доступу: https://delinea.com/blog/privileged-users
7. Агенти привілейованого доступу [Електронний ресурс] – Режим доступу: https://docs.delinea.com/online-help/products/pmgr/current/agents .
8. Win-агенти [Електронний ресурс] – Режим доступу: https://docs.delinea.com/online-help/products/pmgr/current/agents/win .
9. Секретний сервер [Електронний ресурс] – Режим доступу: https://docs.delinea.com/arc/current/secret-server/secret-server-cloud/index.md.
10. Інформаційна панель серевера секретів [Електронний ресурс] – Режим доступу: https://docs.delinea.com/online-help/products/secrets/current/admin/application-dashboard/dashboard-components .
11. Securing-privileged-access https://f.hubspotusercontent10.net/hubfs/19928113/Delinea/ebooks/delinea-ebook-definitive-guide-to-securing-privileged-access.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)